Benutzerhandbuch - Deutsch

FUJITSU

FUJITSU Software ServerView Suite

# Remote Management

## iRMC S4 - integrated Remote Management Controller

Ausgabe August 2015

## Kritik… Anregungen… Korrekturen…

Die Redaktion ist interessiert an Ihren Kommentaren zu diesem Handbuch. Ihre Rückmeldungen helfen uns, die Dokumentation zu optimieren und auf Ihre Wünsche und Bedürfnisse abzustimmen.

Sie können uns Ihre Kommentare per E-Mail an manuals@ts.fujitsu.com senden.

## Zertifizierte Dokumentation nach DIN EN ISO 9001:2000

Um eine gleichbleibend hohe Qualität und Anwenderfreundlichkeit zu gewährleisten, wurde diese Dokumentation nach den Vorgaben eines Qualitätsmanagementsystems erstellt, welches die Forderungen der DIN EN ISO 9001:2000 erfüllt.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

## Copyright und Handelsmarken

Copyright © 2015 Fujitsu Technology Solutions GmbH.

Alle Rechte vorbehalten.
Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle verwendeten Hard- und Softwarenamen sind Handelsnamen und/oder Warenzeichen der jeweiligen Hersteller.

# Inhalt


1 Einleitung . . . . . 13

1.1 Zielgruppen und Zielsetzung des Handbuchs . . . . . 15
1.2 Funktionen des iRMC S4 (Überblick) . . . . . 16
1.3 Benutzeroberflächen des iRMC S4 . . . . . 24
1.4 iRMC S4-gesteuerte LEDs auf dem Frontpanel . . . . . 25
1.5 Kommunikationsprotokolle, die vom iRMC S4 genutzt werden . . . . . 26
1.6 IPMI - Technischer Hintergrund . . . . . 27
1.7 DCMI (Data Center Management Interface) . . . . . 35
1.8 Änderungen gegenüber den vorherigen Ausgaben . . . . . 36
1.9 ServerView Suite Link-Sammlung . . . . . 36
1.10 Dokumentation zur ServerView Suite . . . . . 38
1.11 Darstellungsmittel . . . . . 39

2 Zum ersten Mal am iRMC S4 anmelden . . . . . 41

2.1 Voraussetzungen . . . . . 41
2.2 iRMC S4-Werksvoreinstellungen . . . . . 42
2.3 An der iRMC S4-Weboberfläche anmelden . . . . . 43

3 Konfiguration des iRMC S4 . . . . . 45

3.1 LAN-Schnittstelle des iRMC S4 konfigurieren . . . . . 45
3.1.1 Voraussetzungen . . . . . 46
3.1.1.1 An der richtigen LAN-Schnittstelle gesteckt? . . . . . 46
3.1.1.2 Zusammenspiel der IP-Adressen des iRMC S4 und des Systems . . . . . 47
3.1.1.3 Zugriff aus einem anderen Sub-Netz . . . . . 47
3.1.2 LAN-Schnittstelle konfigurieren Konfiguration-Tools . . . . . 48
3.1.3 LAN-Schnittstelle mit UEFI Setup Utility konfigurieren . . . . . 49
3.1.4 LAN-Schnittstelle testen . . . . . 50

**3.2 Text-Konsolen-Umleitung via LAN über das UEFI Setup Utility konfigurieren . . . 51**
3.2.1 Text-Konsolen-Umleitung für den iRMC S4 konfigurieren . . . 52
3.2.2 Konsolen-Umleitung bei laufendem Betriebssystem nutzen . . . 54

**3.3 Serielle Schnittstelle des iRMC S4 konfigurieren und nutzen . . . 56**
3.3.1 Die serielle Schnittstelle des iRMC S4 konfigurieren . . . 56
3.3.2 Benutzeroberfläche Remote Manager (Serial) nutzen . . . 58

**3.4 iRMC S4 über die iRMC-Weboberfläche konfigurieren . . . 59**
3.4.1 LAN-Parameter konfigurieren . . . 59
3.4.2 Alarmbenachrichtigung (Alerting) konfigurieren . . . 60
3.4.3 Text-Konsolen-Umleitung konfigurieren . . . 60

**4 Benutzerverwaltung für den iRMC S4 . . . 61**

**4.1 Konzept der Benutzerverwaltung für den iRMC S4 . . . 62**

**4.2 Benutzerberechtigungen . . . 65**

**4.3 Lokale Benutzerverwaltung für den iRMC S4 . . . 67**
4.3.1 Lokale Benutzerverwaltung über die iRMC S4-Weboberfläche . . . 67
4.3.2 Lokale Benutzerverwaltung über den Server Configuration Manager . . . 68
4.3.3 SSHv2 Public Key-Authentifizierung für lokale iRMC S4-Benutzer . . . 69
4.3.3.1 Öffentlichen und privaten SSHv2-Schlüssel erzeugen . . . 70
4.3.3.2 Öffentlichen SSHv2-Schlüssel aus Datei auf den iRMC S4 laden. . . . 74
4.3.3.3 PuTTY und OpenSSH Client für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren . . . 76
4.3.3.4 Beispiel: Öffentlicher SSHv2-Schlüssel . . . 81

**5 Advanced Video Redirection (AVR) . . . 83**

**5.1 Voraussetzung: Die Einstellungen für die AVR überprüfen . 84**

**5.2 AVR über ein Java-Applet verwenden . . . 86**
5.2.1 AVR-Fenster . . . 87
5.2.2 Geringe Bandbreite verwenden . . . 88
5.2.3 Parallele AVR-Sitzungen . . . 88

5.2.4 „Lokaler Bildschim Aus Kontrolle“-Funktionalität . . . . . 92
5.2.5 Umleitung der Tastatur . . . . . 93
5.2.6 Umleitung der Maus . . . . . 96
5.2.7 Menüs und Symbolleiste des AVR-Fensters . . . . . 96
5.2.7.1 Menü Video . . . . . 98
5.2.7.2 AVR-Fenster - Menü „Tastatur“ . . . . . 102
5.2.7.3 AVR-Fenster - Menü „Maus“ . . . . . 109
5.2.7.4 AVR-Fenster - Menü „Optionen“ . . . . . 111
5.2.7.5 AVR-Fenster - Menü „Medien“ . . . . . 113
5.2.7.6 AVR -Fenster - Menü „Ein-/Ausschalten“ . . . . . 114
5.2.7.7 AVR -Fenster - Menü „Aktive Benutzer“ . . . . . 116
5.2.7.8 AVR-Fenster - Menü „Hilfe“ . . . . . 116
5.2.7.9 AVR-Symbolleiste . . . . . 118

**5.3 AVR über HTML5 verwenden . . . . . 121**

**6 Virtuelle Medien Wizard . . . . . 123**

**6.1 Virtuelle Medien auf Remote-Workstation bereitstellen . . . 124**
6.1.1 Virtuelle Medien Wizard starten . . . . . 125
6.1.2 Dialog Virtuelle Medien . . . . . 126
6.1.3 Speichermedien für virtuelle Medien bereitstellen . . . . . 128
6.1.4 Virtuelle Medien-Verbindungen löschen . . . . . 131

**7 iRMC-Weboberfläche . . . . . 133**

**7.1 An der iRMC-Weboberfläche anmelden . . . . . 134**

**7.2 Erforderliche Benutzerberechtigungen . . . . . 136**

**7.3 Aufbau der Bedienoberfläche . . . . . 144**

**7.4 System Informationen - Informationen zum Server . . . . . 147**
7.4.1 System Überblick - Allgemeine Informationen zum Server . . . . . 148
7.4.2 System Komponenten Information - Informationen zu den Server-Komponenten . . . . . 154
7.4.3 AIS Connect – AIS Connect konfigurieren und verwenden . . . 157
7.4.4 System Report . . . . . 162
7.4.5 CPU-Auslastungs-Historie . . . . . 164
7.4.6 Netzwerk Anschlüsse . . . . . 166
7.4.7 Driver Monitor . . . . . 167

**7.5 RAID Informationen - Informationen zu den RAID-Systemen . . . . . 168**
7.5.1 RAID Controller - Informationen zu RAID Controllern und verbundenen Batterien . . . . . 169
7.5.2 Festplatteneinheiten – Informationen zu RAID-Festplatteneinheiten . . . . . 171
7.5.3 Festplatten - Informationen zu RAID Physikalische Laufwerke . 175
7.5.4 Logische Laufwerke - Informationen über logische RAID-Laufwerke . . . . . 177

**7.6 BIOS-Einstellungen sichern/wiederherstellen, BIOS aktualisieren . . . . . 179**
7.6.1 BIOS-Parameter und -Einstellungen in Datei sichern / aus Datei wiederherstellen . . . . . 180
7.6.1.1 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format sichern . . . . . 181
7.6.1.2 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format wiederherstellen . . . . . 183
7.6.2 BIOS aktualisieren via "Aktualisierung aus Datei" oder via TFTP . . . . . 185

**7.7 iRMC S4 - Informationen, Firmware und Zertifikate . . . . . 190**
7.7.1 iRMC S4 Informationen – Informationen zum iRMC S4 . . . . 191
7.7.2 iRMC S4 Zeit - Zeitoptionen für den iRMC S4 . . . . . 195
7.7.3 iRMC S4 Firmware Einstellungen abspeichern - Firmware-Einstellungen abspeichern . . . . . 198
7.7.4 Zertifikat Austausch - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden . . . . . 200
7.7.5 Selbstsigniertes Zertifikat erzeugen - Selbstsigniertes RSA Zertifikat erzeugen . . . . . 207
7.7.6 iRMC S4 Firmware Aktualisierung . . . . . 209

**7.8 Energieverwaltung . . . . . 214**
7.8.1 Ein-/Ausschalten - Server ein-/ausschalten . . . . . 215
7.8.2 Energieverwaltungsoptionen - Energieverwaltung des Servers konfigurieren . . . . . 220
7.8.3 Netzteil Information - Stromversorgung und IDPROM-Daten der FRU-Komponenten . . . . . 223

**7.9 Energieverbrauch - Energieverbrauch des Servers steuern . . . . . 224**
7.9.1 Konfiguration der Energieverbrauchssteuerung - Energieverbrauch des Servers konfigurieren . . . . . 225

7.9.2 Aktueller System Energieverbrauch - aktuellen Energieverbrauch anzeigen . . . . . 231
7.9.3 Energieverbrauch Verlauf - zeitlichen Verlauf des Energieverbrauchs anzeigen . . . . . 232

**7.10 Sensoren - Status der Sensoren überprüfen . . . . . 236**
7.10.1 Lüfter - Lüfter überprüfen . . . . . 237
7.10.2 Temperatur - Temperatursensoren überprüfen . . . . . 240
7.10.3 Spannungen - Spannungssensoren überprüfen . . . . . 242
7.10.4 Netzteil - Stromversorgung überprüfen . . . . . 243
7.10.5 Komponenten Status - Status der Serverkomponenten überprüfen . . . . . 245

**7.11 Fehlerspeicher und interner Ereignisspeicher . . . . . 248**
7.11.1 IPMI-Fehlerliste - Information zum Fehlerspeicher und Anzeige der Fehlerspeicher-Einträge . . . . . 250
7.11.2 Interne Ereignisliste - Information zum internen Ereignisspeicher und Anzeige der Einträge . . . . . 253
7.11.3 Fehlerspeicher Konfiguration - IPMI SEL und internen Ereignisspeicher konfigurieren . . . . . 256
7.11.4 Syslog Konfiguration – Syslog-Weiterleitung für den Fehlerspeicher und den internen Ereignisspeicher konfigurieren . . . . . 259

**7.12 Server Management Informationen - Server-Einstellungen konfigurieren . . . . . 263**

**7.13 Netzwerk Einstellungen - LAN-Parameter konfigurieren . . . . . 268**
7.13.1 Netzwerk Schnittstelle - Ethernet-Einstellungen des iRMC S4 konfigurieren . . . . . 269
7.13.2 Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren . . . . . 276
7.13.3 Proxy Einstellungen– Proxyeinstellungen konfigurieren . . . . . 280
7.13.4 DNS Konfiguration - DNS für den iRMC S4 konfigurieren . . . . 282
7.13.5 SNMP Allgemeine Konfiguration . . . . . 286

**7.14 Benachrichtigungen - Alarmbenachrichtigung konfigurieren . . . . . 289**
7.14.1 SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren . . . . . 290
7.14.2 E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren . . . . . 292

**7.15 Benutzerverwaltung . . . . . 299**
7.15.1 Benutzer Verwaltung - lokale Benutzerverwaltung am iRMC S4 . . . . . 299
7.15.1.1 Neuen Benutzer konfigurieren . . . . . 301
7.15.1.2 Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details) . . . . . 302
7.15.2 Verzeichnisdienst Konfiguration (LDAP) - Verzeichnisdienst am iRMC S4 konfigurieren . . . . . 313
7.15.2.1 LDAP-Standardgruppen mit Autorisierungseinstellungen auf dem iRMC S4 . . . . . 316
7.15.2.2 iRMC S4 für Microsoft Active Directory konfigurieren . . . . 323
7.15.2.3 iRMC für Novell eDirectory / OpenLDAP / OpenDS / Open DJ konfigurieren . . . . . 328
7.15.3 Centralized Authentication Service (CAS) Konfiguration - CAS Konfiguration . . . . . 335

**7.16 Konsolen Umleitung - Konsole umleiten . . . . . 341**
7.16.1 BIOS Text Konsole - Textkonsolen-Umleitung konfigurieren und starten . . . . . 341
7.16.1.1 BIOS Konsolen Umleitung Optionen - Textkonsolen-Umleitung konfigurieren . . . . . 342
7.16.1.2 Textkonsolen-Umleitung bei laufendem Betriebssystem nutzen . . . . . 344
7.16.2 Advanced Video Redirection - Advanced Video Redirection (AVR) starten . . . . . 346

**7.17 Virtual Media . . . . . 356**
7.17.1 Virtual Media Optionen - Virtuelle Medien-Optionen konfigurieren . . . . . 357
7.17.2 Dezentrale Medien - Remote-ISO-Images verbinden . . . . . 359

**7.18 Lifecycle Management . . . . . 363**
7.18.1 Aktualisierungs Einstellungen – allgemeine eLCM-Update-Einstellungen konfigurieren . . . . . 365
7.18.2 Online Aktualisierung – eLCM-Online-Aktualisierung konfigurieren . . . . . 366
7.18.3 Offline Aktualisierung – eLCM-Offline-Aktualisierung konfigurieren . . . . . 372
7.18.4 Custom Image – benutzerdefinierte Images verwenden . . . . 378
7.18.5 PrimeCollect – Health Management . . . . . 383

8 iRMC S4 über Telnet/SSH (Remote Manager) . . . . . 387

8.1 Voraussetzung am verwalteten Server . . . . . 387
8.2 Remote Manager bedienen . . . . . 388
8.3 Menü-Übersicht . . . . . 389
8.4 Anmeldeprozess . . . . . 392
8.5 Hauptmenü des Remote Manager . . . . . 394
8.6 Erforderliche Benutzerberechtigungen . . . . . 396
8.7 Passwortwort ändern . . . . . 398
8.8 System Informationen - Informationen zum verwalteten Server . . . . . 398
8.9 Power Management . . . . . 399
8.10 Enclosure Information - Systemeventlog und Status der Sensoren . . . . . 400
8.11 Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S4 . . . . . 404
8.12 RAID Management . . . . . 405
8.13 Console Redirection (EMS/SAC) - Text-Konsolen-Umleitung starten . . . . . 406
8.14 Start a Command Line shell... - SMASH CLP Shell starten . . . . . 406
8.15 Console Logging - Meldungsausgabe auf die Text-Konsole (seriell) . . . . . 407
8.16 Command Line Protocol (CLP) . . . . . 409

9 iRMC S4 via Server Configuration Manager konfigurieren . 413

9.1 Server Configuration Manager via ServerView Installation Manager aufrufen . . . . . 415
9.2 Server Configuration Manager über das Windows Startmenü aufrufen . . . . . 415
9.3 Server Configuration Manager über den Operations Manager aufrufen . . . . . 417

**10 Firmware aktualisieren . . . . . 421**

**10.1 Firmware des iRMC S4 (Überblick) . . . . . 422**

**10.2 USB Memory Stick erstellen . . . . . 424**

**10.3 Firmware-Images aktualisieren . . . . . 427**
10.3.1 Update über die iRMC S4-Weboberfläche . . . . . 428
10.3.2 Update via ServerView Update Manager . . . . . 428
10.3.3 Online-Update via ServerView Update Manager Express oder ASP . . . . . 429
10.3.4 Update mit den Betriebssystem-Flash-Tools . . . . . 430
10.3.5 Update über das Menü der FlashDisk . . . . . 432

**10.4 Emergency Flash . . . . . 434**

**10.5 Flash-Tools . . . . . 435**

**11 Remote-Installation des Betriebssystems via iRMC S4 . . . 439**

**11.1 Betriebssystem via iRMC S4 installieren - generelles Vorgehen . . . . . 440**

**11.2 Speichermedium als Virtual Media verbinden . . . . . 442**

**11.3 Verwalteten Server von der ServerView Suite DVD 1 booten und via Installation Manager konfigurieren . . . . . 444**

**11.4 Betriebssystem nach Konfiguration auf dem verwalteten Server installieren . . . . . 448**
11.4.1 Windows nach Konfiguration auf dem verwalteten Server installieren . . . . . 448
11.4.2 Linux nach Konfiguration auf dem verwalteten Server installieren . . . . . 450

**12 Anhang . . . . . 453**

**12.1 Vom iRMC S4 unterstützte IPMI OEM-Kommandos . . . . . 453**
12.1.1 Überblick . . . . . 453
12.1.2 Beschreibung der IPMI OEM-Kommandos . . . . . 455
12.1.2.1 Beschreibungsformat . . . . . 455
12.1.2.2 SCCI-konforme Power On/Off-Kommandos . . . . . 456
12.1.2.3 SCCI-konforme Kommunikationskommandos . . . . . 461
12.1.2.4 SCCI-konformes Signalkommando . . . . . 463

12.1.2.5 Firmware-spezifische Kommandos . . . 464
12.1.2.6 BIOS-spezifische Kommandos . . . 468
12.1.2.7 iRMC S4-spezifische Kommandos . . . 470

**12.2 iRMC S4 mit SCCI und per Skript-Konfiguration konfigurieren . . . 481**
12.2.1 iRMC S4-Konfigurationsdaten . . . 481
12.2.1.1 Überblick . . . 481
12.2.1.2 SCCI-Dateiformat . . . 483
12.2.1.3 Einschränkungen . . . 487
12.2.1.4 Konfigurationsdaten des iRMC S4 exportieren/importieren . 488
12.2.2 Skript-Konfiguration des iRMC S4 . . . 489
12.2.2.1 Liste der vom iRMC S4 unterstützten SCCI-Kommandos . . 489
12.2.2.2 Skripte mit cURL . . . 490
12.2.2.3 Skripte mit Visual Basic (VB) Script . . . 491
12.2.2.4 Skripte mit Python . . . 492
12.2.2.5 Verschlüsselte Kennwörter mit dem Programm iRMC_PWD.exe generieren . . . 493

**12.3 iRMC S4-System-Report . . . 496**
12.3.1 Download per Skript und automatische Bewertung des iRMC S4-Reports . . . 496
12.3.1.1 Skripte mit cURL . . . 496
12.3.1.2 Skripterstellung mit Visual Basic . . . 497
12.3.2 Informationsabschnitte . . . 498
12.3.2.1 Liste der unterstützten System Report-Abschnitte in der XML-Datei . . . 498
12.3.2.2 Abschnitt "Summary" . . . 498
12.3.2.3 BIOS . . . 500
12.3.2.4 Processor . . . 500
12.3.2.5 Memory . . . 501
12.3.2.6 Fans . . . 502
12.3.2.7 Temperature . . . 502
12.3.2.8 Power Supplies . . . 502
12.3.2.9 Voltages . . . 503
12.3.2.10 IDPROMS . . . 503
12.3.2.11 SensorDataRecords . . . 503
12.3.2.12 PCIDevices . . . 503
12.3.2.13 SystemEventLog . . . 504
12.3.2.14 InternalEventLog . . . 504
12.3.2.15 BootStatus . . . 505
12.3.2.16 ManagementControllers . . . 506

# 1 Einleitung

Moderne Serversysteme werden zunehmend komplexer. Entsprechend steigen auch die Anforderungen an das Management dieser Systeme.

Als Reaktion auf diese Entwicklung gründeten einige Hersteller die Initiative „Intelligent Platform Management Interface (IPMI)“ mit dem Ziel der Definition einer standardisierten, abstrakten und Mitteilung-basierten Schnittstelle zwischen dem zentralen System-Controller (Baseboard Management Controller -BMC) und intelligenter Hardware zum Plattform-Management. Näheres zu IPMI finden Sie im Abschnitt "IPMI - Technischer Hintergrund" auf Seite 27.

Der **i**ntegrated **R**emote **M**anagement **C**ontroller iRMC ist ein BMC mit integrierter LAN-Verbindung und erweiterter Funktionalität. Auf diese Weise bietet der iRMC die umfassende Kontrolle von PRIMERGY Servern, unabhängig vom Systemstatus. Insbesondere ermöglicht der iRMC das "Out-of-Band"-Management (Lights-out-Management, LOM) von PRIMERGY Servern. Für das Out-of-Band-Management wird ein dedizierter Managementkanal genutzt, über den der Systemadministrator den Server via Fernüberwachung verwalten kann, egal, ob der Server ein- oder ausgeschaltet ist.

Bild 1: iRMC S4 auf dem System Board eines PRIMERGY Servers

Als autonomes System auf dem System Board eines aktuellen PRIMERGY Servers verfügt der iRMC über ein eigenes Betriebssystem, einen eigenen Webserver sowie eine eigene Benutzerverwaltung und ein eigenständiges Alarm-Management. Der iRMC wird auch im Stand-by-Betrieb des Servers mit Strom versorgt.

Neben der Möglichkeit des Out-of-Band-Managements von PRIMERGY Servern unterstützen die erweiterten Funktionen der neuesten Version des iRMC, der mit einer integrierten SD-Karte ausgestattet ist, eine umfassende Lebenszyklusverwaltung von PRIMERGY Servern. Da die Lebenszyklusverwaltung weitgehend in den iRMC integriert ("eingebettet") ist und vollständig von diesem gesteuert wird, wird diese Komponente als "embedded Life Cycle Management (eLCM)" bezeichnet.

Zur Verwendung einiger eLCM-Funktionen muss der iRMC mit dem ServerView Agentless Service kommunizieren und zusammenarbeiten, der auf dem verwalteten Server ausgeführt wird. Durch die Kommunikation mit dem ServerView Agentless Service erhält der iRMC S4 außerdem zusätzliche In-Band-Informationen.

Im vorliegenden Handbuch werden Konfiguration und Bedienoberflächen des iRMC beschrieben.

# 1.1 Zielgruppen und Zielsetzung des Handbuchs

Das Handbuch wendet sich an Systemverwalter, Netzverwalter und Service-Fachleute, die über fundierte Hard- und Software-Kenntnisse verfügen. Es vermittelt Grundkenntnisse zur Technologie von IPMI und informiert ausführlich über folgende Themen:

- Anmelden am iRMC
- Konfiguration des iRMC
- Benutzerverwaltung am iRMC
- Grafische Konsolen-Umleitung (Advanced Video Redirection) via iRMC
- Virtuelle Medien via iRMC
- iRMC-Weboberfläche
- Telnet/SSH-basierte Oberfläche (Remote Manager) des iRMC
- Konfiguration des iRMC über den Server Configuration Manager
- Firmware-Aktualisierung
- Remote-Installation des Betriebssystems via iRMC
- Anhang IPMI OEM-Kommandos
  - IPMI OEM-Kommandos
  - iRMC mit SCCI und per Skript-Konfiguration konfigurieren

### Service

Falls Sie weitere Fragen zum Remote Management für PRIMERGY-Server haben, wenden Sie sich an Ihren zuständigen Service und Supportpartner.

### Weitere Informationen

*http://www.ts.fujitsu.com*

# 1.2 Funktionen des iRMC S4 (Überblick)

Der iRMC S4 unterstützt eine Vielzahl von standardmäßig angebotenen Funktionen. Mit der grafischer Konsolen-Umleitung (Advanced Video Redirection, AVR) und Virtual Media bietet der iRMC S4 außerdem zwei zusätzliche, fortschrittliche Leistungsmerkmale für das Remote Management von PRIMERGY Servern. Für die Nutzung von AVR, Virtual Media und embedded Lifecycle Management (eLCM) benötigen Sie einen gültigen Lizenzschlüssel (License Key), den Sie käuflich erwerben können.

**Standardfunktionalität des iRMC S4**

- Browser-Zugang

  Der iRMC S4 verfügt über einen eigenen Webserver, der von der Management-Station über einen Standard-Webbrowser angesprochen werden kann.

- Sicherheit (SSL, SSH)

  Der Zugang zum Webserver kann, ebenso wie die grafische Konsolen-Umleitung inklusive Maus und Tastatur, über HTTPS/SSL abgesichert werden. Für den Zugriff auf den iRMC S4 über den Remote Manager kann eine kryptografisch gesicherte Verbindung eingerichtet werden, die durch die Mechanismen von SSH abgesichert ist. Der Remote Manager ist eine alphanumerische Bedienoberfläche des iRMC S4.

- ServerView-Integration

  Die ServerView Agents erkennen den iRMC S4 und ordnen ihn automatisch dem betreffenden Server zu. Damit lässt sich die iRMC S4-Weboberfläche ebenso wie die Textkonsolen-Umleitung über das ServerView Remote Management Frontend direkt aus dem ServerView Operations Manager heraus starten.

  Die Kommunikation zwischen dem iRMC S4 und dem ServerView Agentless Service (ab ServerView Operations Manager 7.0) ermöglicht ein erweitertes Out-of-Band-Management von PRIMERGY Servern.

- Energieverwaltung (Power Management)

  Unabhängig vom Systemzustand haben Sie folgende Möglichkeiten, vom Remote-Arbeitsplatz aus den verwalteten Server ein- und auszuschalten:

  – via iRMC S4-Weboberfläche
  – über den Remote Manager und das Command Line Interface (CLP)
  – per Script

- Steuerung des Energieverbrauchs (Power Consumption Control)

  Der iRMC S4 ermöglicht eine umfassende Energieverbrauchssteuerung am verwalteten Server. Darüber hinaus können Sie den Modus festlegen (minimaler Stromverbrauch oder maximale Performance), nach dem der iRMC S4 den Energieverbrauch am verwalteten Server regelt. Zwischen diesen Modi können Sie beliebig umschalten.

- Customer Self Service (CSS)

  An der iRMC S4-Weboberfläche informieren die Übersichtstabellen zu Server-Komponenten, Sensoren und Stromversorgung in einer gesonderten Spalte, ob es sich bei der betreffenden Server-Komponente um eine CSS-Komponente handelt. Ferner zeigt der Fehlerspeicher (System Eventlog, SEL) in der Fehlerliste für jedes Ereignis an, ob das betreffende Ereignis von einer CSS-Komponente ausgelöst wurde.

- Text-Konsolen-Umleitung

  Über das ServerView Remote Management Frontend können Sie eine Telnet/SSH-Sitzung am iRMC S4 starten. Es wird dann der Remote Manager aufgerufen, über den Sie eine Text-Konsolumleitung starten können.

- Grundfunktionen eines BMC

  Der iRMC S4 unterstützt die Grundfunktionen eines BMC wie Spannungsmonitoring, Event-Logging und Recovery-Kontrolle.

- „Headless“ Systembetrieb

  Maus, Bildschirm und Tastatur sind am verwalteten Server nicht erforderlich. Daraus resultieren Vorteile, wie niedrigere Kosten, wesentlich einfachere Verkabelung im Rack und höhere Sicherheit.

- Identifizierungs-LED

  Zur einfacheren Identifizierung eines Systems, z.B. in einem voll ausgebauten Rack, können Sie über die iRMC S4-Weboberfläche die Identifizierungs-LED einschalten.

- Fehler-LED (Gobal Error-LED)

  Eine Fehler-LED informiert Sie jederzeit über den Status des verwalteten Systems und liefert zugleich den CSS (Customer Self Service)-Status.

- Stromversorgungs-LED

  Die Stromversorgungs-LED zeigt an, ob der Server gerade eingeschaltet oder ausgeschaltet ist.

- S5-LED

  Die S5-LED informiert Sie über die Energieversorgung des Servers.

- CIM-Unterstützung

  Der iRMC S4 unterstützt CIM-XML, WS-Man und Smash-CLP.

- LAN

  Bei einigen Systemen ist die LAN-Schnittstelle der eingebauten System-Netzkarte (Network Interface Card) des Servers dediziert für das Management LAN reserviert. Bei anderen Systemen können Sie diese LAN-Schnittstelle per Konfiguration wahlweise

  – für das Management LAN reservieren,
  – für den „Shared“-Betrieb mit dem System einrichten oder
  – ganz dem System zur Verfügung stellen.

  Dem iRMC S4 zugeordnet sind die Ports, die mit dem Symbol eines Schraubenschlüssels gekennzeichnet sind (siehe Bild 7 auf Seite 47).

- Netzwerk-Bonding

  Das Netzwerk-Bonding für den iRMC S4 wurde für den Fall eines Ausfalls von Ethernet-Netzwerkadaptern für Redundanz konzipiert. Daher ist der Datenverkehr für das iRMC S4-Netzwerk-Management vor Serviceausfällen geschützt, die beim Ausfall einer einzelnen physischen Verbindung auftreten können.

  Der iRMC S4 unterstützt den aktiven Backup-Modus, d. h. ein Port ist aktiv, bis die Verbindung ausfällt, dann übernimmt der andere Port die MAC und wird aktiv.

- Unterstützung von SNMPv1/v2c/v3

  Sie können auf dem iRMC S4 einen SNMP-Dienst konfigurieren, der SNMPv1/v2c/v3 GET-Anforderungen auf SNMP SC2 MIB (Sc2.mib), SNMP MIB-2, SNMP OS.MIB und SNMP STATUS.MIB unterstützt.

  Wenn der SNMP-Dienst aktiviert ist, können Informationen auf Geräten wie Lüfter, Temperatur-Sensoren etc. direkt "Out-of-Band" vom iRMC S4 auf ein beliebiges System bereitgestellt werden, auf welches ein SNMP Manager läuft.

- Command Line Interface (CLP)

  Der iRMC S4 unterstützt neben dem Remote Manager auch das von der DMTF (Distributed Management Task Force) standardisierte SMASH CLP (**S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol)

- Einfache Konfiguration - interaktiv oder skript-basiert

  Für die Konfiguration des iRMC S4 stehen folgende Tools zur Verfügung:

  – iRMC-Weboberfläche
  – Server Configuration Manager
  – UEFI BIOS Setup

  Die Konfiguration via Server Configuration Manager oder IPMIVIEW können Sie auch skript-basiert durchführen. Auf diese Weise kann bei der ersten Konfiguration des Servers mit dem ServerView Installation Manager auch der iRMC S4 konfiguriert werden. Auch die gleichzeitige Konfiguration einer größeren Anzahl von Servern lässt sich Skript-basiert durchführen.

- Unterstützung des LocalView Service Panels

  Bei PRIMERGY Servern, die über ein ServerView Local Service Panel verfügen, können Sie an diesem Modul erkennen, welches Bauteil defekt ist und ob Sie das defekte Bauteil selbst austauschen können.

- Lokale Benutzerverwaltung

  Der iRMC S4 verfügt über eine eigene Benutzerverwaltung, mit der bis zu 16 Benutzer mit Kennwörtern angelegt und je nach Gruppenzugehörigkeit mit unterschiedlichen Rechten versehen werden können.

- Globale Benutzerverwaltung mithilfe eines Verzeichnisdienstes

  Die globalen Benutzerkennungen für den iRMC S4 werden zentral abgelegt im Verzeichnis (Directory) eines Verzeichnisdienstes. Auf diese Weise lassen sich die Benutzerkennungen auf einem zentralen Server verwalten. Die Benutzerkennungen können somit von allen iRMC S4s verwendet werden, die mit diesem Server im Netz verbunden sind.

  Für die iRMC S4-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – OpenDS

- CAS-basierte Single sign-on (SSO)-Authentifizierung

  Der iRMC S4 unterstützt die Konfiguration des zentralisierten Authentifizierungsdienstes CAS (Centralized Authentication Service). Damit können Sie die iRMC -Weboberfläche für die CAS-basierte Single sign-on (SSO)-Authentifizierung konfigurieren.

  Wenn sich ein Benutzer das erste Mal bei einer Anwendung (z.B. iRMC S4-Weboberfläche) innerhalb der SSO-Domäne des CAS anmeldet, fordert ihn das CAS-spezifische Login-Fenster zur Eingabe seiner Authentisierungsdaten auf. Nach einmaliger erfolgreicher Authentifizierung durch den CAS Service hat der Benutzer dann Zugriff auf die iRMC S4-Weboberfläche sowie auf alle weiteren Services innerhalb der SSO-Domäne, ohne dass er jedes Mal erneut zur Eingabe seiner Authentisierungsdaten aufgefordert wird.

- DNS / DHCP

  Der iRMC S4 unterstützt die automatische Netz-Konfiguration. Er hat einen Default-Namen und DHCP-Unterstützung ist standardmäßig eingestellt, sodass der iRMC S4 seine IP-Adresse vom DHCP-Server erhält. Der iRMC S4-Name wird vom Domain Name System (DNS) registriert. Es werden bis zu fünf DNS-Server unterstützt. Falls DNS/DHCP nicht verfügbar ist, unterstützt der iRMC S4 auch statische IP-Adressen.

- Stromversorgung

  Die Stromversorgung des iRMC S4 erfolgt über die Stand-by-Versorgung des Systems.

- Alarm-Management

  Das Alarm-Management des iRMC S4 bietet folgende Möglichkeiten für die Weiterleitung von Alarmen (Alerting):

  – Platform Event Traps (PET) werden via SNMP versendet.
  – Direkte Benachrichtigung per E-Mail.

  Darüber hinaus versorgt der iRMC S4 die ServerView Agents mit allen relevanten Informationen.

- Fehlerspeicher (System Eventlog, SEL) auslesen, filtern und speichern.

  Den Inhalt des Fehlerspeichers können Sie filtern, einsehen, speichern und löschen

  – über die iRMC S4-Weboberfläche oder

  – über die Telnet/SSH-basierte Schnittstelle (Remote Manager) des iRMC S3.

- Internen Ereignisspeicher (Internal Eventlog) auslesen, filtern und speichern.

  Den Inhalt des internen Ereignisspeichers können Sie filtern, einsehen, speichern und löschen

  – über die iRMC S4-Weboberfläche oder

  – über die Telnet/SSH-basierte Schnittstelle (Remote Manager) des iRMC S4.

- UEFI-Unterstützung

  Unified Extensible Firmware Interface (UEFI) ist die Spezifikation für ein Software-Programm, das die Firmware eines Computers mit seinem Betriebssystem verbindet. UEFI hat einen Firmware-Validierungsprozess, genannt Secure Boot. Secure Boot definiert, wie die Firmware einer Plattform Sicherheitszertifikate, Firmware-Validierung und die Schnittstelle (Protokoll) zwischen Firmware und dem Betriebsssystem verwaltet.

### Erweiterte Funktionalität des iRMC S4

Neben der Standardfunktionalität unterstützt der iRMC S4 zusätzlich die Funktionen „Grafische Konsolen-Umleitung“ (Advanced Video Redirection) und „Virtual Media“.

- Advanced Video Redirection (AVR)

  Der iRMC S4 unterstützt die grafische Konsolen-Umleitung mit folgenden Vorteilen:

  – Bedienung über einen Standard-Webbrowser. Auf der Management-Station braucht außer dem Java Runtime Environment keine zusätzliche Software installiert zu werden.

  – System-unabhängige Weiterleitung von Grafik- und Text-Konsole (einschließlich Maus und Tastatur).

  – Fernzugriff für die Überwachung des System-Neustarts sowie für BIOS-Administration und Bedienung des Betriebssystems.

  – Die grafische Konsolen-Umleitung unterstützt bis zu zwei gleichzeitige „virtuelle Verbindungen“ für das Arbeiten an einem Server von einem anderen Standort aus. Außerdem minimiert die grafische Konsolen-Umleitung die Netzbelastung durch Hardware- und Video-Komprimierung.

  – „Lokaler Bildschirm Aus“ (Local Monitor Off)-Unterstützung: Während einer AVR-Sitzung kann der lokale Bildschirm des verwalteten PRIMERGY Servers ausgeschaltet werden, um Unbefugte daran zu hindern, Eingaben und Aktionen der AVR -Sitzung am Server-lokalen Bildschirm zu verfolgen.

  – Geringe Bandbreite

    Für den Fall, dass nur eine eingeschränkte Datentransfer-Rate verfügbar ist, können Sie für die Dauer Ihrer aktuellen AVR-Sitzung eine geringere Bandbreite (Bits pro Pixel, BPP) hinsichtlich der Farbtiefe konfigurieren.

- Virtuelle Medien

  Mithilfe der Funktion „Virtuelle Medien“ wird ein „virtuelles“ Laufwerk zur Verfügung gestellt, das sich auf einer remoten Workstation befindet, oder es wird zentral mithilfe von *Dezentrale Medien Abbilder verbinden* im Netzwerk verfügbar gemacht.

Die per „Virtuelle Medien“ verfügbaren „virtuellen“ Laufwerke sind ähnlich den lokalen Laufwerken einfach zu verwalten und bieten folgende Möglichkeiten:

- Daten lesen und schreiben.
- Von virtuellen Medien booten.
- Treiber und kleinere Anwendungen installieren.
- BIOS Update vom Remote-Arbeitsplatz durchführen (BIOS update via USB)

Virtual Media unterstützt für die Bereitstellung eines „virtuellen“ Laufwerks am Remote-Arbeitsplatz folgende Gerätetypen:

- CD-ROM
- DVD-ROM
- Memory Stick
- Disketten-Image
- CD-ISO-Image
- DVD-ISO-Image
- Physikalisches Festplattenlaufwerk
- HDD-ISO-Image

Die Funktionalität *Dezentrale Medien Abbilder verbinden* stellt ISO-Images zentral in einem Netzlaufwerk als „virtuelles Laufwerk“ zur Verfügung.

- embedded Lifecycle Management (eLCM)

  Durch die Integration einer umfassenden Funktion zur Lebenszyklusverwaltung in die Firmware des aktuellen iRMC S4 ermöglicht es Ihnen die eLCM-Lösung (embedded Lifecycle Management) der FUJITSU ServerView Suite, die Lebenszyklusverwaltung von PRIMERGY Servern mit wenigen Mausklicks zentral über die iRMC-Weboberfläche zu steuern, ohne dass hierfür physische Geräte eingesetzt werden müssen.

  Die vom iRMC S4 bereitgestellte eLCM-Lösung beinhaltet die folgenden Funktionen:

  - eLCM Update Management
  - eLCM Image Management (Custom Image)
  - eLCM Health Management (PrimeCollect)

  Weitere Informationen hierzu erhalten Sie im Handbuch "ServerView embedded Lifecycle Management (eLCM)".

## 1.3 Benutzeroberflächen des iRMC S4

Der iRMC S4 bietet folgende Kommunikationsschnittstellen:

- **iRMC S4-Weboberfläche (Web-Schnittstelle)**

  Die Verbindung zum iRMC-Webserver erhalten Sie über einen Standard-Webbrowser (z. B. Microsoft Internet Explorer, Mozilla Firefox).

  Über die Weboberfläche des iRMC S4 haben Sie u.a. Zugriff auf alle Systeminformationen und Informationen der Sensoren wie Lüfterdrehzahlen, Spannungen etc. Sie können die Text-basierte Konsolen-Umleitung konfigurieren oder die grafische Konsolen-Umleitung (Advanced Video Redirection, AVR) starten. Darüber hinaus kann der Administrator die komplette Konfiguration des iRMC S4 über die Weboberfläche abwickeln. Der Zugang zum Webserver des iRMC S4 kann über HTTPS/SSL abgesichert werden.

  Die Bedienung des iRMC S4 über die Weboberfläche ist beschrieben im Kapitel "iRMC-Weboberfläche" auf Seite 133.

- **Remote Manager: Text-basierte Telnet/SSH-Oberfläche über LAN**

  Den Remote Manager können Sie wahlweise aufrufen

  – über das ServerView Remote Management Frontend,
  – direkt über einen Telnet/SSH-Client.

  Über die alphanumerische Bedienoberfläche des Remote Manager haben Sie u.a. Zugriff auf System-und Sensorinformationen, das Power Management und den Error-Eventlog. Außerdem können Sie die Textkonsolen-Umleitung sowie eine SMASH CLP Shell starten. Wenn Sie den Remote Manager über SSH (Secure Shell) aufrufen, ist die Verbindung zwischen Remote Manager und verwaltetem Server kryptographisch gesichert.

  Die Bedienung des iRMC S4 über den Remote Manager ist beschrieben im Kapitel "iRMC S4 über Telnet/SSH (Remote Manager)" auf Seite 387.

- **Remote Manager (Serial): Text-basierte Schnittstelle über Serial 1**

  Die Oberfläche des Remote Manager (Serial) ist identisch mit der Oberfläche des Remote Manager.

# 1.4 iRMC S4-gesteuerte LEDs auf dem Frontpanel

Der iRMC S4 steuert die Status-LEDs auf dem Frontpanel des Servers. Die LEDs und ihre Anordnung ist unterschiedlich abhängig vom Servertyp.

**Status-LEDs auf dem Frontpanel (Nexperience design):**

| Status des Servers | LED auf dem Server | |
|---|---|---|
| | S5-LED (gün) | Stromversorgungs-LED (gün) |
| AC-OFF | Aus | Aus |
| S5 (shutdown) | Ein | Aus |
| S0 (power on) | Aus | Ein |
| S3 (sleep mode) | Aus | blinkt mit 1 Hz (vom BIOS gesteuert) |
| iRMC not ready | Ein | blinkt mit 0,5 Hz (vom iRMC gesteuert) |
| Power-on Delay | Ein | Ein |

**Status-LEDs auf dem Frontpanel (legacy design):**

| Status des Servers | Stromversorgungs-LED auf dem Server |
|---|---|
| AC-OFF | Aus |
| S5 (shutdown) | orange |
| S0 (power on) | grün |
| S3 (sleep state) | blinkt grün mit 1 Hz (vom BIOS gesteuert) |
| iRMC not ready | blinkt abwechselnd in orange/grün mit 1 Hz (vom iRMC gesteuert) |
| Power-on Delay | gelb |

# 1.5 Kommunikationsprotokolle, die vom iRMC S4 genutzt werden

In Tabelle 1 sind die vom iRMC verwendeten Kommunikationsprotokolle aufgelistet:

| Gegenseite der Verbindung | Kommunikationsrichtung | iRMC S4-Seite der Verbindung (Portnummer / Protokoll) | Konfigurierbar | Standardmäßig aktiviert |
|---|---|---|---|---|
| RMCP | → | 623/UDP | nein | ja |
| | ← | 623/UDP | | |
| HTTP port | → | 80/TCP | ja | ja |
| | ← | 80/TCP | | |
| HTTPs port | → | 443/TCP | ja | ja |
| | ← | 443/TCP | | |
| Telnet | → | 3172/TCP | ja | nein |
| | ← | 3172/TCP | | |
| SSH | → | 22/TCP | ja | ja |
| | ← | 22/TCP | | |
| SNMP (general mess.) | → | 161/UDP | nein | nein |
| | ← | 161/UDP | | |
| SNMP Trap | → | 162/UDP | nein | ja |
| LDAP | → | 389/TCP/UDP | ja | nein |
| | ← | 389/TCP/UDP | | |
| LDAP SSL | → | 636/TCP/UDP | ja | nein |
| | ← | 636/TCP/UDP | | |
| Email / SMTP | → | 25/TCP | ja | nein |
| | ← | 25/TCP | | |
| CIM | → | 5988/CIM-XML | | |
| | ← | 5989/CIM-XML | | |
| | → | 80/WS-MAN | | |
| | ← | 80/WS-MAN | | |

Tabelle 1: Kommunikationsprotokolle, die vom iRMC S4 genutzt werden

# 1.6 IPMI - Technischer Hintergrund

Über die IPMI-Schnittstelle stellt der iRMC S4 die BMC-Funktionalität zur Verfügung.

### Intelligent Platform Management

Die Initiative „Intelligent Platform Management“ ist eine Reaktion auf die ansteigende Komplexität moderner Serversysteme. Zahlreiche Hersteller haben sich in dieser Initiative zusammengeschlossen, um eine neue Lösung für die Überwachung dieser Serversysteme zu erarbeiten.

Der Begriff „Intelligent Platform Management“ bringt den Kernaspekt dieses Lösungsansatzes zum Ausdruck: Funktionen zum Überwachen und Wiederherstellen von Systemen werden direkt in die Hard- und Firmware für das Plattform-Management implementiert.

### Ziel

Ziel war die Definition einer standardisierten, abstrakten und Mitteilung-basierten Schnittstelle zwischen dem zentralen System-Controller (Baseboard Management Controller - BMC) und intelligenter Hardware zum Plattform-Management.

Dabei fassten die Standardisierungsgremien die zentralen Charakteristika verschiedener Baugruppen zum Plattform-Management in standardisierende Beschreibungen.

### Definition

Die IPMI-Spezifikation definiert:

“IPMI is a hardware level interface specification that is ‘management software neutral’ providing monitoring and control functions that can be exposed through standard management software interfaces such as DMI, WMI, CIM, SNMP, etc. As a hardware level interface, it sits at the bottom of a typical management software stack” [siehe Abschnitt "IPMI und andere Management-Standards" auf Seite 28].

### Vorteil

Die IPMI-Spezifikationen sichern die Unabhängigkeit der Funktionen zu Inventory, Logging, Recovery und Überwachung eines Systems vom Prozessor, BIOS oder Betriebssystem des Systems.

Damit kann ein System auch in das Plattform-Management einbezogen werden, wenn es heruntergefahren und ausgeschaltet ist.

### IPMI und andere Management-Standards

Am besten kann IPMI genutzt werden in Verbindung mit einer Software zum System-Management, die unter dem Betriebssystem läuft. Mit der Integration der IPMI-Funktionalität in die Managementfunktionalität, die eine Management-Applikation und das Betriebssystem bieten, entsteht eine mächtige Umgebung zum Plattform-Management.

Eine Übersicht zum Verhältnis von IPMI zum Management-Software-Stack zeigt Bild 2:

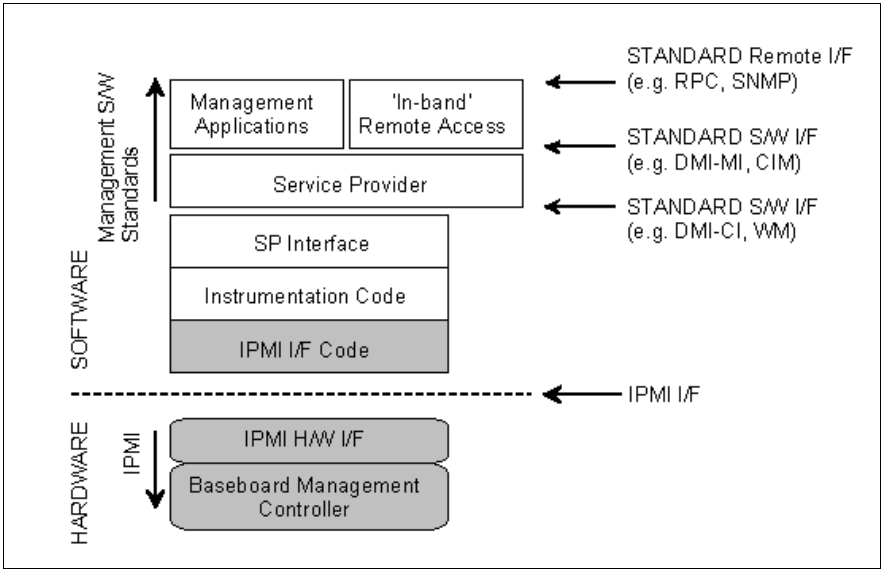



Bild 2: IPMI im Management-Software-Stack (Quelle: IPMI-Spezifikation, siehe Abschnitt "Referenzen" auf Seite 35)

### IPMI, IPMB und ICMB

Im Rahmen der IPMI-Initiative entstanden drei zentrale Standards:

– *IPMI. Intelligent Platform Management Interface Specification*
beschreibt die übergeordnete Architektur, die gängigen Kommandos, Ereignisformate, Datenpakete und Eigenschaften, die in IPMI-basierten Systemen zum Einsatz kommen.

– *IPMB. Intelligent Platform Management Bus*
ist ein $I^2C$-basierter (write only) Bus, der eine standardisierte Verbindung herstellt zwischen verschiedenen Baugruppen in einem Gehäuse.
Der IPMB kann auch als standardisierte Schnittstelle für Remote-Management-Baugruppen eingesetzt werden.

– *ICMB. Intelligent Chassis Management Bus*
(Derzeit im ServerView Remote Management-Umfeld nicht implementiert.) bietet eine standardisierte Schnittstelle für den Austausch von Information zum Plattform-Management und zur Kontrolle zwischen Systemen. ICMB ist so entworfen, dass er mit einem Gerät implementiert werden kann, das an den IPMB angeschlossen wird.

### IPMI Implementierung

Kernelement einer IPMI-Implementierung ist der Baseboard Management Controller (BMC).
Der BMC erfüllt folgende Aufgaben:

– Der BMC organisiert die Schnittstelle zwischen der Software für das System-Management und der Hardware für das Plattform-Management.

– Er bietet autonome Funktionen für die Überwachung, das Event-Logging und die Recovery-Kontrolle.

– Der BMC dient als Gateway zwischen der Software zum System-Management und IPMB.

IPMI ermöglicht das Erweitern von Plattform-Management: Über den IPMB können zusätzliche Management-Controller angebunden werden. Der IPMB ist ein $I^2C$-basierter serieller Bus, der zwischen den Hauptmodulen des Systems verläuft. Er wird für die Kommunikation mit und zwischen den Management-Controllern genutzt.

Mit der Unterstützung mehrerer Management-Controller bietet IPMI eine skalierbare Architektur: Ein komplexes Server-System kann mehrere Controller für die Überwachung verschiedener Subsysteme nutzen, z.B. der Stromversorgungen, der hot-swap RAID-Laufwerkseinschübe, usw.

Darüberhinaus bietet IPMI 'low-level' $I^2C$-Kommandos, mit denen über einen am IPMB angeschlossenen Management-Controller zugegriffen werden kann auf 'unintelligente' $I^2C$-Baugruppen, die keine IPMI-Kommandos verarbeiten.

Einen Überblick über die grundlegenden Elemente einer IPMI-Implementierung bietet Ihnen Bild 3 auf Seite 31.

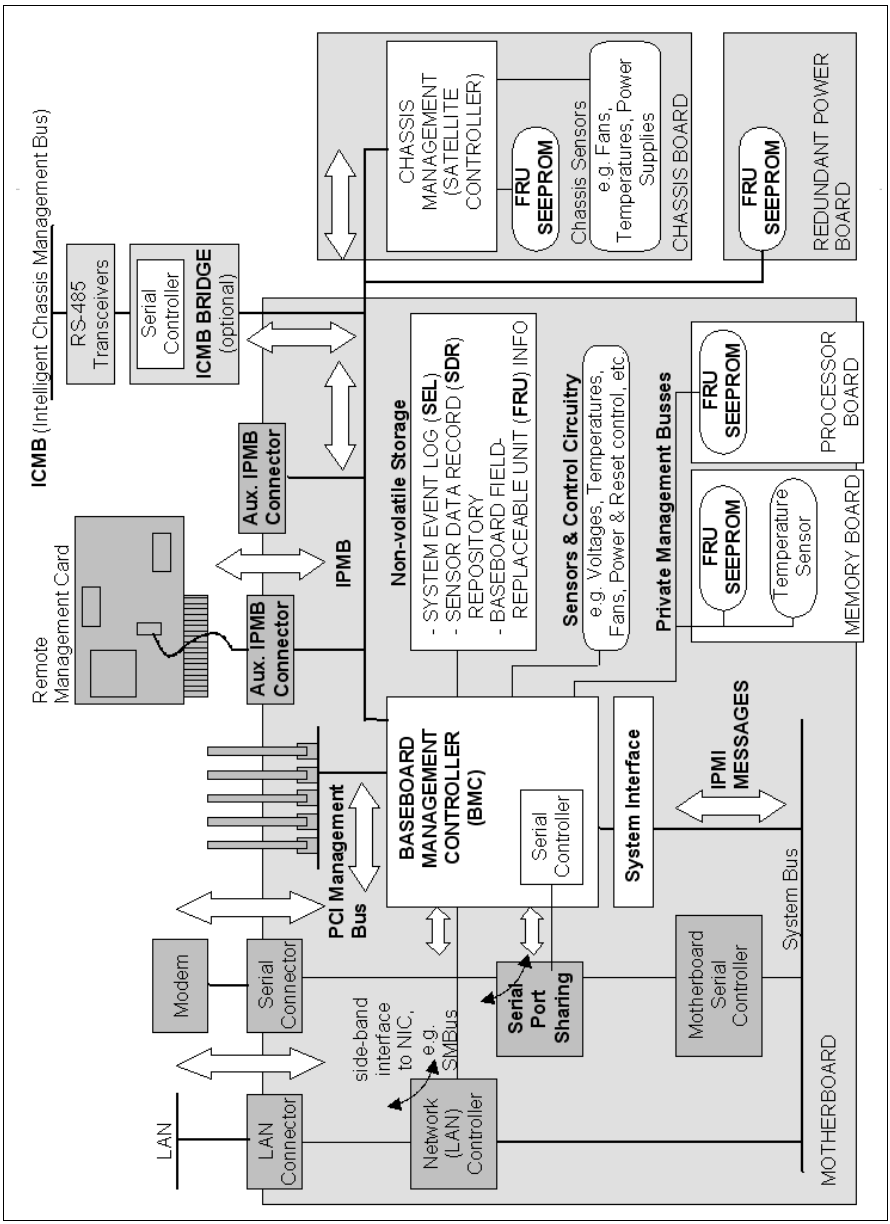



Bild 3: IPMI-Blockdiagramm (Quelle: IPMI-Spezifikation, siehe Abschnitt "Referenzen" auf Seite 35)

### IPMI und „in-band“ und „out-of-band“ Management

Im System-Management-Umfeld wird unterschieden zwischen „in-band“-Management und „out-of-band“-Management:

– „in-band“-Management findet statt, wenn das Betriebssystem am verwalteten Server läuft.

– „out-of-band“-Management findet statt, wenn das Betriebssystem am verwalteten Server nicht läuft, z.B. weil Hardware defekt ist.

Mit den verschiedenen Schnittstellen, die ein IPMI-fähiges System zur Verfügung stellt, lassen sich IPMI-fähige Systeme sowohl „in-band“ als auch „out-of-band“ verwalten.

### IPMI-over-LAN

“IPMI-over-LAN” ist die gängige Bezeichung für die Spezifikation der LAN-Schnittstelle im IPMI-Standard. Diese Spezifikation legt fest, wie IPMI-Mitteilungen an bzw. von dem BMC eines verwalteten Systems gesendet werden können - verkapselt in RMCP (Remote Management Control Protocol)-Datenpakete. Diese RMCP-Datenpakete werden übertragen über eine Ethernet-LAN-Verbindung über das UDP (User Datagram Protocol) unter IPv4 (Internet Protocol Version 4).

Das RMCP-Protokoll wurde spezifiziert, um das Management von Systemzuständen zu unterstützen, in denen das Betriebssystem nicht läuft. Das RMCP ist ein einfaches Frage-Antwort-Protokoll.

Die Schnittstelle für eine solche Verbindung wird bereitgestellt über einen onboard LAN-Controller, der dem BMC zugeordnet ist.

Die Schnittstelle kann nur über einen onboard LAN-Controller zur Verfügung gestellt werden, nicht über eine gesteckte LAN-Karte.

Von den zwei Ports, die RCMP unter UDP nutzt, kommuniziert der BMC mit dem LAN-Controller über den Port 623 (Primary RMCP Port).

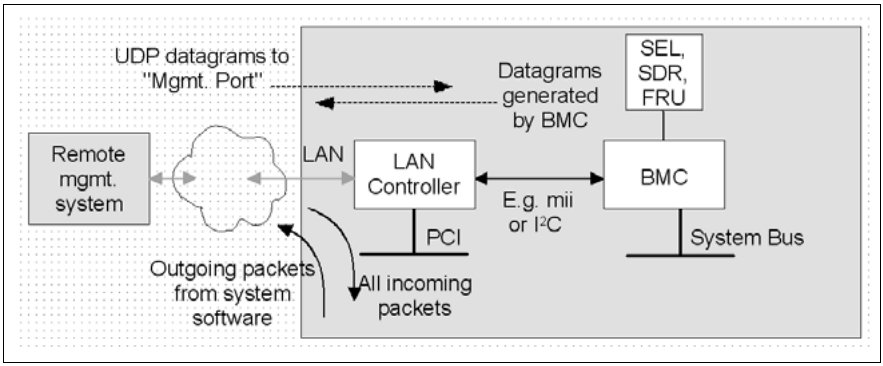



Bild 4: BMC und LAN-Controller

**Serial Over LAN-Schnittstelle (SOL)**

"Serial Over LAN" ist eine Schnittstelle im IPMI V2.0-Standard, die die Übertragung serieller Daten über eine LAN-Verbindung regelt. Im Einzelnen spezifiziert SOL dabei die Paketformate und Protokolle für den LAN-Transfer serieller Datenströme zwischen dem Serial Controller am verwalteten Rechner und einem Remote-Arbeitsplatz. SOL basiert auf der IPMI-over-LAN-Spezifikation.

Zur Einrichtung einer SOL-Verbindung initiiert eine Remote-Management-Anwendung zunächst eine IPMI-over-LAN-Session mit dem BMC. Danach können die SOL-Dienste vom Remote-Arbeitplatz aus aktiviert werden. Der Datenverkehr zwischen dem Serial Controller und dem Remote-Arbeitsplatz wird über dieselbe IPMI-Session abwickelt, über die auch die IPMI-Kommandos abgewickelt werden.

Sobald eine SOL-Verbindung eingerichtet ist, verläuft der Datentransfer zwischen Serial Controller und Remote Arbeitsplatz nach folgendem Schema:

– Transfer vom Serial Controller an den Remote-Arbeitsplatz:
  Der vom Serial Controller ausgehende Datenstrom wird vom BMC partitioniert, in Pakete "verpackt" und über LAN an den Remote-Arbeitsplatz gesendet.

– Transfer vom Remote-Arbeitsplatz an den Serial Controller:
  Die Zeichen, die in den vom Remote-Arbeitsplatz gesendeten Paketen enthalten sind, werden vom BMC entpackt und als Zeichenstrom an den Serial Controller weitergeleitet.

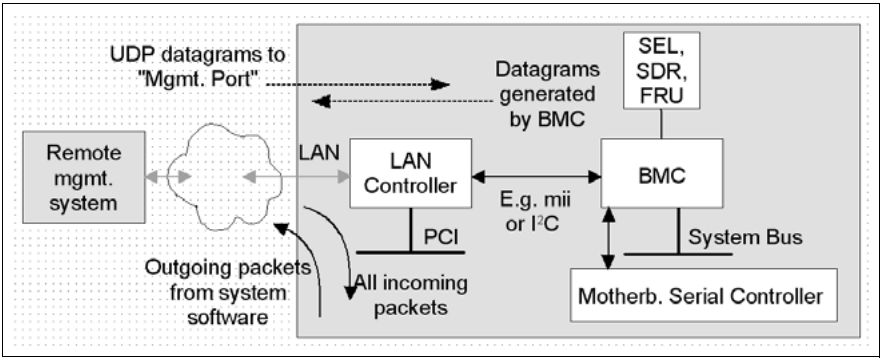



Bild 5: BMC und SOL

Die SOL-Zeichendaten werden als SOL-Mitteilungen zwischen dem BMC des verwalteten Systems und dem Remote-Arbeitsplatz ausgetauscht. Verkapselt in RMCP+-Datenpakete werden SOL-Mitteilungen in UDP Datagrammen übertragen über eine Ethernet-LAN-Verbindung unter IPv4 (Internet Protocol Version 4). Das RMCP+-Protokoll basiert auf dem RMCP-Protokoll, enthält jedoch Erweiterungen u.a. für Verschlüsselung und Authentifizierung.

Serial Over LAN ermöglicht "headless" Management durch Konsolumleitung sowohl des BIOS als auch des Betriebssystems des verwalteten Servers. Kostenintensive Konzentratorlösungen werden nicht benötigt.

### Kanal-Konzept unter IPMI

'Kanäle' stellen die Mechanismen zur Verfügung, mit denen IPMI-Meldungen über verschiedene Verbindungsträger zum BMC geleitet werden. Es können bis zu neun Kanäle unterstützt werden. Die Systemschnittstelle und der Primary IPMB sind festgelegt. Die anderen sieben Kanäle stehen der Implementierung offen.

Kanäle können 'session-based' oder 'session-less' sein. Das 'session'-Konzept hat zwei Bedeutungen: Es ist entweder ein Konzept zur Benutzer-Authentifizierung (siehe Abschnitt "Benutzerkennungen" auf Seite 35) oder ein Konzept, um mehrere IPMI-Meldungsströme über einen einzelnen Kanal zu leiten.

Beispiele für ’session-based’ Kanäle sind LAN-Kanäle oder serielle oder Modem-Kanäle. Beispiele für ’session-less’ Kanäle sind die Systemschnittstelle und der IPMB.

### Benutzerkennungen

Für ’session-based’ Kanäle (siehe Abschnitt "Kanal-Konzept unter IPMI" auf Seite 34) ist eine Nutzeranmeldung notwendig. Die ’session-less’ Kanäle haben dagegen keine Benutzer-Authentifizierung.

Unter IPMI ist die Konfiguration der Benutzer Kanal-spezifisch. So kann ein Benutzer verschiedene Rechte haben, je nachdem ob er auf den BMC über den LAN-Kanal oder über den seriellen Kanal zugreift.

### Referenzen

Informationen zu den IPMI-Standards finden Sie im Internet:

*http://developer.intel.com/design/servers/ipmi/index.htm*

## 1.7 DCMI (Data Center Management Interface)

Der iRMC S4 unterstützt das DCMI (Data Center Management Interface)-Protokoll, das konform zum IPMI V2.0-Standard ist. Ziel von DCMI ist es, Administrierbarkeit und Energieeffizienz von Servern in großen Datencentern zu optimieren.

Zur Unterstützung des Hardware-Managements von Servern in Datencentern bietet DCMI u.a. folgende Schlüsselfunktionen:

- Inventory-Funktionen (Server-Identifikation)
- Energieverwaltung und -überwachung
- Überwachung und Steuerung des Energieverbrauchs
- Event-Logging
- Temperaturüberwachung

Detaillierte Informationen finden Sie auf der DCMI-Hompage:

*http://www.intel.com/technology/product/DCMI*

## 1.8 Änderungen gegenüber den vorherigen Ausgaben

Dieses Handbuch bezieht sich auf die iRMC S4 **Firmware Version 8.0** und löst das folgende Online-Handbuch ab: “iRMC S4 - integrated Remote Management Controller”, Ausgabe April 2015.

Das Handbuch enthält folgende Erweiterungen:

- iRMC-Weboberfläche
  - Neue Umleitungsfunktion via HTML5 parallel zur Java-basierten Umleitung
  - Neue HP SIM-Integration
  - CIM-Unterstützung

    Mit dem Common Information Model (CIM) können Beziehungsinformationen (was ist womit verbunden) genutzt werden, um die Quelle und den Status bei Problemen zu verfolgen.
- Erweiterte SNMP-Unterstützung
- RESTful API

  REST (REpresentational State Transfer) ist ein Architekturstil, der sich an die Kommunikation annähert, wie sie bei der Entwicklung von Webdiensten stattfindet. Wenn Webdienste REST-Architektur verwenden, werden sie RESTful APIs (Application Programming Interfaces) oder REST APIs genannt. REST-Architektur bezieht das Lesen einer bezeichneten Webseite ein, die eine XML-Datei enthält.

## 1.9 ServerView Suite Link-Sammlung

Fujitsu Technology Solutions stellt Ihnen über die Link-Sammlung zahlreiche Downloads und weiterführende Informationen zur ServerView Suite und zu PRIMERGY Servern zur Verfügung.

Zur ServerView Suite werden Ihnen Links zu folgenden Themen angeboten:

- Forum
- Service Desk
- Handbücher

- Produktinformationen
- Sicherheitsinformationen
- Software Downloads
- Schulungen

Die Downloads umfassen u.a.:

– Aktuelle Software-Stände zur ServerView Suite sowie ergänzende Readme-Dateien.

– Informationsdateien und Aktualisierungsdateien (Update Sets) für systemnahe Software-Komponenten (BIOS, Firmware, Treiber, ServerView Agents und ServerView-Update-Agenten) zur Aktualisierung der PRIMERGY Server anhand des ServerView Update Managers oder für den lokalen Update einzelner Server anhand des ServerView Update Managers Express.

– Die aktuellen Versionen aller Dokumentationen zur ServerView Suite

Die Downloads können kostenlos vom Fujitsu Technology Solutions Webserver heruntergeladen werden.

Zu PRIMERGY Servern werden Ihnen Links zu folgenden Themen angeboten:

- Service Desk
- Handbücher
- Produktinformationen
- Ersatzteilkatalog

**Zugriff auf die Link-Sammlung**

Die Link-Sammlung der ServerView Suite erreichen Sie über verschiedene Wege:

1. Über den ServerView Operations Manager.

   ► Wählen Sie auf der Startseite bzw. in der Menüzeile *Help – Links* aus.

   Die Startseite der ServerView Suite Link-Sammlung wird angezeigt.

2. Über die Startseite der Online-Dokumentation zur ServerView Suite auf dem Manual-Server von Fujitsu Technology Solutions.

   Sie gelangen auf die Startseite der Online-Dokumentation mit folgendem Link:

*http://manuals.ts.fujitsu.com*

- ► Wählen Sie links in der Auswahlliste *x86 Servers* aus.
- ► Klicken Sie rechts unter *Ausgewählte Dokumente* auf *PRIMERGY ServerView Links*.

Die Startseite der ServerView Suite Link-Sammlung wird angezeigt.

3. Über die ServerView Suite DVD 2
   - ► Markieren Sie im Startfenster der ServerView Suite DVD 2 die Option *Select ServerView Software Products*.
   - ► Klicken Sie auf *Start*. Sie gelangen auf die Seite der Software Produkte der ServerView Suite.
   - ► Wählen Sie in der Menüleiste *Links*.

   Die Startseite der ServerView Suite Link-Sammlung wird angezeigt.

## 1.10 Dokumentation zur ServerView Suite

Die Dokumentation für die ServerView Suite ist über das Internet als Download kostenlos erhältlich. Die Online-Dokumentation finden Sie unter *http://manuals.ts.fujitsu.com* und dem Link *x86 servers*.

# 1.11 Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet:

| | |
|---|---|
| **Warnung** | Mit diesem Symbol wird auf Gefahren hingewiesen, die zu Gesundheitsgefährdung, Datenverlust und Geräteschäden führen können. |
| | Mit diesem Symbol werden wichtige Informationen und Tipps hervorgehoben. |
| ► | Mit diesem Symbol wird ein Arbeitsschritt, den Sie ausführen müssen, dargestellt. |
| *Kursive Schrift* | Im Fließtext werden Kommandos, Menüpunkte, die Namen von Schaltflächen, Optionen, Variablen, Dateinamen und Pfadnamen *kursiv* dargestellt. |
| <Schrift> | Kennzeichnet Variablen, die durch aktuelle Werte ersetzt werden müssen. |
| `dicktengleich` | Ausgaben des Systems werden `dicktengleich` dargestellt. |
| **`Dicktengleich halbfett`** **`Dicktengleich halbfett`** | Über die Tastatur einzugebende Anweisungen werden dicktengleich halbfett dargestellt. |
| [eckige Klammern] | Kennzeichnen optionale Eingaben. |
| {geschweifte Klammern} | Kennzeichnen eine Liste Alternativen, die durch „\|“ voneinander getrennt sind. |
| Tasten symbole | Tasten werden entsprechend ihrer Abbildung auf der Tastatur dargestellt. Wenn explizit Großbuchstaben eingegeben werden sollen, so wird die Shift-Taste angegeben, z.B. SHIFT - A für A.<br><br>Müssen zwei Tasten gleichzeitig gedrückt werden, so wird dies durch einen Bindestrich zwischen den Tastensymbolen gekennzeichnet. |

Tabelle 2: Darstellungsmittel

Wird auf Textstellen in diesem Handbuch verwiesen, so wird die Überschrift des Kapitels bzw. Abschnitts genannt, wobei sich die Seitenangabe auf den Beginn des Abschnitts bezieht.

# 2 Zum ersten Mal am iRMC S4 anmelden

Der iRMC S4 bietet Voreinstellungen, mit denen Sie sich ohne weitere Konfigurationsschritte das erste Mal am iRMC S4 anmelden können.

## 2.1 Voraussetzungen

**Am Remote-Arbeitsplatz:**

– Windows: Internet Explorer ab Version 10.x.
  Linux: Mozilla Firefox 3.x.

– Für die Konsolumleitung:
  Sun Java Virtual Machine 1.6 oder in einer höheren Version.

**In Ihrem Netz:**

– Im Ihrem Netz muss sich ein DHCP-Server befinden.

– Wenn Sie sich an der iRMC-Weboberfläche an Stelle einer IP-Adresse über einen symbolischen Namen anmelden möchten, muss der DHCP-Server in Ihrem Netz für dynamisches DNS konfiguriert sein.

– DNS muss konfiguriert sein. Andernfalls müssen Sie die IP-Adresse erfragen.

## 2.2 iRMC S4-Werksvoreinstellungen

Die Firmware des iRMC S4 stellt eine Standard-Administratorkennung und einen Standard-DHCP-Namen für den iRMC S4 zur Verfügung.

**Standard-Administratorkennung:**

*Administratorkennung*: admin

*Passwort*: admin

Für Administratorkennung und Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

Aus Sicherheitsgründen wird empfohlen, nach der ersten Anmeldung eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Kennwort zu ändern (siehe Abschnitt "Benutzerverwaltung" auf Seite 299).

**Standard-DHCP-Name für den iRMC S4**

Der Standard-DHCP-Name für den iRMC S4 folgt dem Muster: *IRMC<Seriennummer>*

Die Seriennummer entspricht den letzten 3 Bytes der MAC-Adresse des iRMC S4. Die MAC-Adresse des iRMC S4 können Sie dem Aufkleber auf Ihrem PRIMERGY Server entnehmen.

Nach dem Anmelden finden Sie die MAC-Adresse des iRMC S4 als unveränderlichen Eintrag oberhalb der Eingabefelder in der Seite *Netzwerk Schnittstelle* (siehe Seite 269).

## 2.3 An der iRMC S4-Weboberfläche anmelden

► Öffnen Sie am Remote-Arbeitsplatz einen Webbrowser und geben Sie den DNS-Namen oder die IP-Adresse des iRMC S4 ein.

Den DNS-Namen des iRMC S4 können Sie dem Aufkleber auf Ihrem PRIMERGY Server entnehmen.

Es wird dann der folgende Anmeldebildschirm angezeigt:

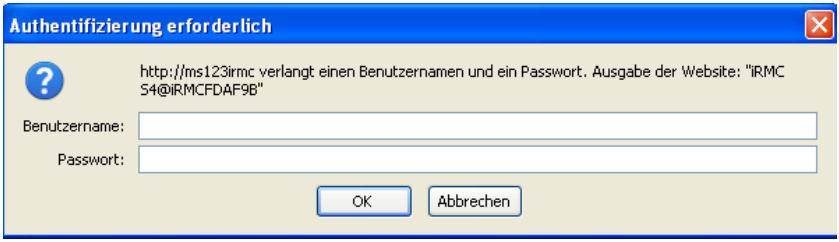



Bild 6: Anmeldebildschirm der iRMC S4-Weboberfläche

Falls kein Anmeldebildschirm angezeigt wird, überprüfen Sie die LAN-Verbindung (siehe Abschnitt "LAN-Schnittstelle testen" auf Seite 50).

► Geben Sie die Daten der Standard-Administratorkennung ein:

*Benutzername*: admin

*Kennwort*: admin

► Klicken Sie auf *OK*, um die Einträge zu bestätigen.

Die iRMC-Weboberfläche öffnet sich, die Seite *System Information* (siehe Seite 147) wird angezeigt.

# 3 Konfiguration des iRMC S4

**Für die Konfiguration des iRMC S4 stehen folgende Tools zur Verfügung:**

– UEFI Setup Utility (siehe Seite 49)

– iRMC Weboberfläche (siehe Seite 133)

– Server Configuration Manager (siehe Seite 413)

**Dieses Kapitel informiert über folgende Themen:**

– LAN-Schnittstelle des iRMC S4 über das UEFI Setup Utility konfigurieren (siehe Seite 49).

– Text-Konsolen-Umleitung via LAN über das UEFI Setup Utility konfigurieren (siehe Seite 51).

– Serielle Schnittstelle des iRMC S4 über das UEFI Setup Utility konfigurieren (siehe Seite 56).

– iRMC S4 über die Weboberfläche konfigurieren (Überblick, siehe Seite 59).

## 3.1 LAN-Schnittstelle des iRMC S4 konfigurieren

Dieser Abschnitt beschreibt:

– Voraussetzungen für die Konfiguration der LAN-Schnittstelle

– LAN-Schnittstelle im UEFI Setup Utility konfigurieren

– LAN-Schnittstelle testen

Für den Switch-Port zum Anschluss des iRMC S4 muss „Spanning Tree“ deaktiviert sein (z.B. Port Fast=enabled; Fast Forwarding=enabled).

## 3.1.1 Voraussetzungen

Beachten Sie folgende Voraussetzungen für das Konfigurieren der IP-Adresse:

– Die LAN-Verbindung muss am richtigen Port gesteckt sein (siehe Abschnitt "An der richtigen LAN-Schnittstelle gesteckt?" auf Seite 46)

– Zusammenspiel der IP-Adressen des iRMC S4 und des Systems (siehe Abschnitt "Zusammenspiel der IP-Adressen des iRMC S4 und des Systems" auf Seite 47).

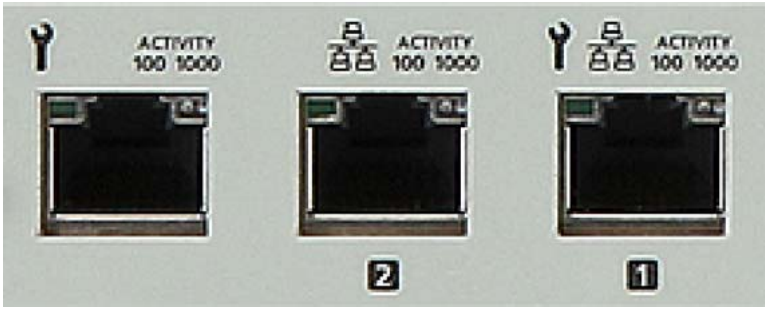
### 3.1.1.1 An der richtigen LAN-Schnittstelle gesteckt?

Die Schnittstelle für eine LAN-Verbindung wird bereitgestellt über einen onboard LAN-Controller, der dem iRMC S4 zugeordnet ist (siehe Bild 4 auf Seite 33).

Die Systembaugruppe eines PRIMERGY Servers stellt je nach Typ des Servers zwei oder drei LAN-Schnittstellen zur Verfügung. Dem iRMC S4 zugeordnet sind die Ports, die mit dem Symbol eines Schraubenschlüssels gekennzeichnet sind (in Bild 7 sind dies Port 1 und der linke obere Port).

Prüfen Sie, ob die LAN-Verbindung am richtigen Port gesteckt ist!

Je nach Typ des PRIMERGY Servers können unterschiedliche Ports mit dem Schraubenschlüssel-Symbol gekennzeichnet sein.




Dediziertes Service / Management LAN

(Port exklusiv reserviert für den iRMC S4; mit dem iRMC S4 ist eine LAN Geschwindigkeit bis zu 1000 MBit/s verfügbar (abhängig von der Server Hardware). (1)

Shared LAN
(iRMC S4 und System)

(2) LAN (Port ist exklusiv für das System reserviert.)

Bild 7: Ports für den iRMC S4 (mit Schraubenschlüssel-Symbol gekennzeichnet)

#### 3.1.1.2 Zusammenspiel der IP-Adressen des iRMC S4 und des Systems

Der LAN-Controller des PRIMERGY Servers verlangt eine eigene IP-Adresse für den iRMC S4, um eine sichere Zustellung von Datenpaketen an den iRMC S4 (und nicht an das Betriebssystem) zu gewährleisten.

Die IP-Adresse des iRMC S4 muss sich von der des Systems (Betriebssystems) unterscheiden.

#### 3.1.1.3 Zugriff aus einem anderen Sub-Netz

Wenn der Remote-Arbeitsplatz aus einem anderen Sub-Netz auf den iRMC S4 des verwalteten Servers zugreift und kein DHCP verwendet wird, müssen Sie das Gateway konfigurieren.

### 3.1.2 LAN-Schnittstelle konfigurieren Konfiguration-Tools

Je nach Server-Typ können Sie die LAN-Schnittstelle des iRMC S4 wahlweise wie folgt konfigurieren:

Abhängig vom Typ des PRIMERGY Servers

– über das UEFI Setup Utility (siehe Seite 49)

– iRMC S4-Weboberfläche (siehe Abschnitt "Netzwerk Einstellungen - LAN-Parameter konfigurieren" auf Seite 268),

– über den Server Configuration Manager (siehe Kapitel "iRMC S4 via Server Configuration Manager konfigurieren" auf Seite 413).

### 3.1.3 LAN-Schnittstelle mit UEFI Setup Utility konfigurieren

Die LAN-Schnittstelle Ihres iRMC S4 können Sie mit dem UEFI Setup Utility konfigurieren:

- Rufen Sie das UEFI Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.
- Rufen Sie das Menü *iRMC LAN parameter configuration* auf:

  *Server Mgmt – iRMC LAN Parameters Configuration*

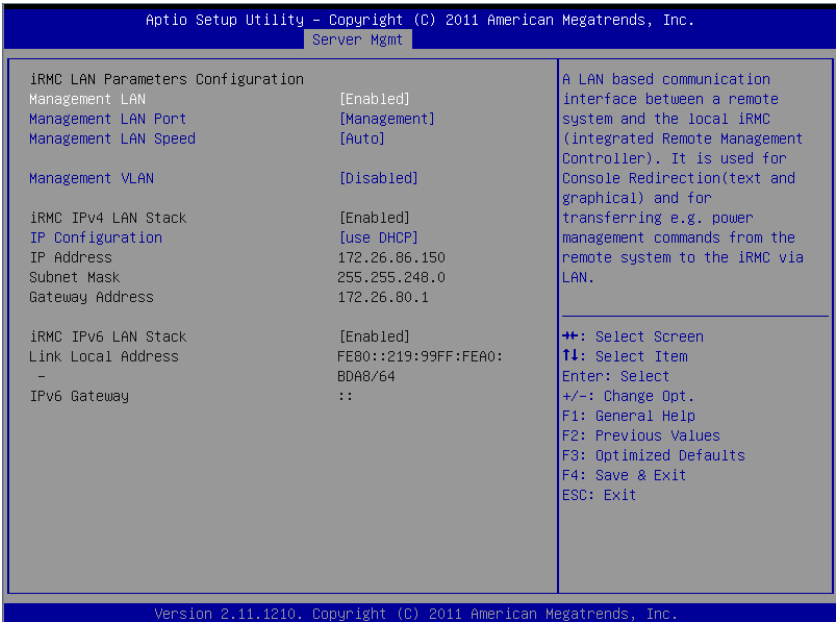

Aptio Setup Utility – Copyright (C) 2011 American Megatrends, Inc.
Server Mgmt
iRMC LAN Parameters Configuration
Management LAN [Enabled]
Management LAN Port [Management]
Management LAN Speed [Auto]
Management VLAN [Disabled]
iRMC IPv4 LAN Stack [Enabled]
IP Configuration [use DHCP]
IP Address 172.26.86.150
Subnet Mask 255.255.248.0
Gateway Address 172.26.80.1
iRMC IPv6 LAN Stack [Enabled]
Link Local Address FE80::219:99FF:FEA0:
- BDA8/64
IPv6 Gateway ::
A LAN based communication interface between a remote system and the local iRMC (integrated Remote Management Controller). It is used for Console Redirection(text and graphical) and for transferring e.g. power management commands from the remote system to the iRMC via LAN.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.11.1210. Copyright (C) 2011 American Megatrends, Inc.

Bild 8: Menü iRMC LAN Parameters Configuration

- Konfigurieren Sie folgende Einstellungen:

  *Management LAN*
  Setzen Sie die Einstellung auf *Enabled*.

  *Management LAN Port*
  Es wird die Einstellung *Management* empfohlen.

  Für die Konfiguration der restlichen Einstellungen siehe Abschnitt "Netzwerk Einstellungen - LAN-Parameter konfigurieren" auf Seite 268 und/oder konsultieren Sie das für Ihren Server relevante Handbuch "BIOS (Aptio) Setup Utility".

- Sichern Sie die Einstellungen.
- Wenn Sie die Konsolen-Umleitung über den iRMC S4 nutzen möchten, fahren Sie fort mit Abschnitt "Text-Konsolen-Umleitung für den iRMC S4 konfigurieren" auf Seite 52.

  Wenn Sie die Text-Konsolen-Umleitung über den iRMC S4 nicht nutzen möchten, beenden Sie das UEFI Setup und fahren Sie fort mit dem nachfolgenden Abschnitt "LAN-Schnittstelle testen".

### 3.1.4 LAN-Schnittstelle testen

Für LAN-Schnittstelle können Sie wie folgt testen:

- Versuchen Sie sich über einen Webbrowser an der iRMC-Weboberfläche anzumelden. Falls Sie keine Anmeldungssaufforderung erhalten, funktioniert die LAN-Schnittstelle wahrscheinlich nicht.
- Testen Sie die Verbindung zum iRMC S4 mit einem Ping-Kommando.

## 3.2 Text-Konsolen-Umleitung via LAN über das UEFI Setup Utility konfigurieren

Je nach Konfiguration der Text-Konsolen-Umleitung und Betriebssystem des Servers steht die Text-Konsolen-Umleitung zur Verfügung

– nur für die Dauer der BIOS POST-Phase oder

– über die BIOS POST-Phase hinaus auch bei laufendem Betriebssystem

Dieser Abschnitt beschreibt:

– Konfiguration der Text-Konsolen-Umleitung via LAN über das UEFI Setup Utility

– Betriebssystem-spezifische Besonderheiten, die Sie beachten müssen, wenn Sie die Konsolen-Umleitung auch bei laufendem Betriebssystem nutzen wollen.

Die Text-Konsolen-Umleitung via LAN können Sie auch über die iRMC-Weboberfläche konfigurieren (siehe Abschnitt "BIOS Text Konsole - Textkonsolen-Umleitung konfigurieren und starten" auf Seite 341).

## 3.2.1 Text-Konsolen-Umleitung für den iRMC S4 konfigurieren

- ► Rufen Sie das UEFI Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.
- ► Rufen Sie das Menü *Server Mgmt* auf:

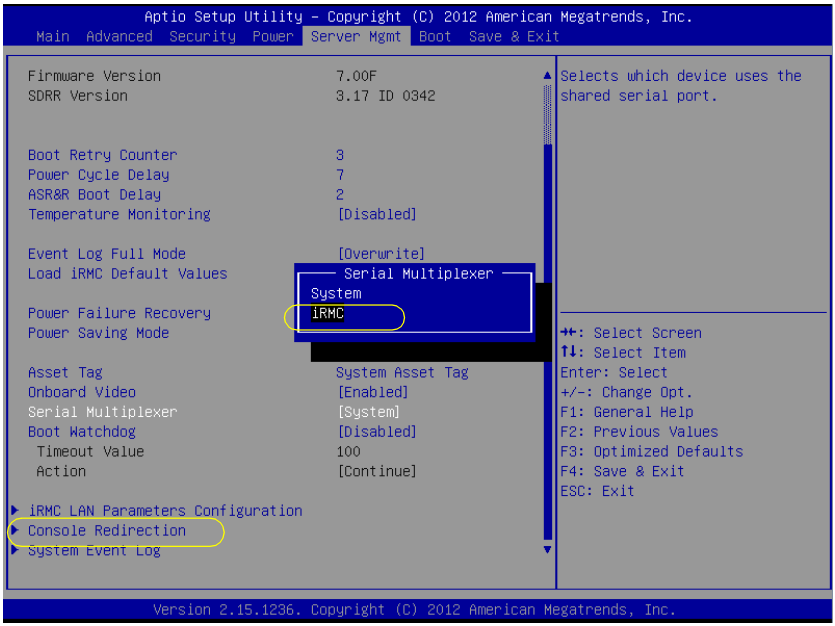



Bild 9: Menü Server Mgmt

- ► Konfigurieren Sie die folgenden Einstellungen:

*Serial Multiplexer*
Setzen Sie die Einstellung auf *iRMC*.

► Rufen Sie das Menü *Console Redirection* auf:

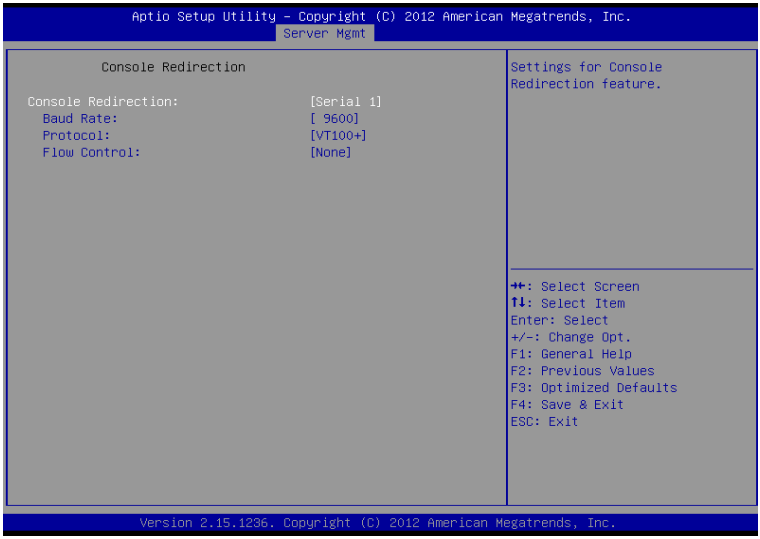



Bild 10: Menü Console Redirection

► Konfigurieren Sie im Menü *Console Redirection* folgende Einstellungen:

*Console Redirection*
: Setzen Sie den Wert auf *Serial 1*. Das Terminal verwendet dann die erste seriell Schnittstelle.

*Baud Rate*
: Legen Sie die Baud-Rate fest.

*Protocol*
: Lassen Sie diese Einstellung unverändert. (Die Einstellung hängt vom verwendeten Terminal-Typ ab.)

*Flow Control*
: Die Einstellung hängt vom verwendeten Terminal-Typ ab. Die Einstellungen müssen immer am Terminal und am verwalteten Server gleich sein.

### UEFI Setup beenden

► Sichern Sie die Einstellungen und beenden Sie das UEFI Setup Utility.

► Fahren Sie fort mit Abschnitt "LAN-Schnittstelle testen" auf Seite 50.

## 3.2.2 Konsolen-Umleitung bei laufendem Betriebssystem nutzen

Sie können - je nach Betriebssystem des verwalteten Servers - auch nach der BIOS POST-Phase noch die Konsolen-Umleitung nutzen.

### Windows Server 2008 / 2012

Wenn die Konsolen-Umleitung bereits während der Windows-Installation aktiviert wird, wird Sie im Rahmen der Windows-Installation automatisch konfiguriert.

Wenn die Konsolen-Umleitung erst nach Abschluss der Windows-Installation aktiviert wird, muss sie „von Hand“ konfiguriert werden.

Windows Server 2008/2012 verarbeitet die Konsolen-Umleitung nach der POST-Phase automatisch. Weitere Einstellungen sind nicht notwendig. Während der Boot-Phase des Betriebssystems wird die SAC-Konsole von Windows Server übertragen:

140.100.100.231 RX200-S2-1 [SP 140.100.100.231:23] (Connected)
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: The CMD command is now available.
SAC>

Bild 11: SAC-Konsole von Windows Server

### Linux

Ein Linux-Betriebssystem müssen Sie konfigurieren, damit es die Konsolen-Umleitung nach der POST-Phase übernimmt. Wenn es konfiguriert ist, haben Sie vom Remote-Arbeitplatz aus vollen Zugriff.

### Notwendige Einstellungen

Die Einstellungen können sich je nach Programmversion etwas ändern.

Sie sollten die Version Ihres Betriebssystems prüfen. Falls die Version von den Versionen abweicht, für die nachfolgend die Einstellungen beschriebenen sind, informieren Sie sich bitte in der Dokumentation zu Ihrem Betriebssystem.

*SuSE und RedHat*

Fügen Sie am Ende der Datei */etc/inittab*: folgende Zeile an

```
xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0
```

*RedHat*

Fügen Sie in die Datei */etc/grub.conf* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baud-rate> console=tty0
```

*SuSE*

Fügen Sie in die Datei */boot/grub/menu.lst* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baud-rate> console=tty0
```

# 3.3 Serielle Schnittstelle des iRMC S4 konfigurieren und nutzen

Über die serielle Schnittstelle des iRMC S4 können Sie die Terminal-Anwendung Remote Manager (Serial) über ein Nullmodemkabel verwenden (siehe Abschnitt "Benutzeroberfläche Remote Manager (Serial) nutzen" auf Seite 58).

## 3.3.1 Die serielle Schnittstelle des iRMC S4 konfigurieren

- Rufen Sie das UEFI Setup Utility des verwalteten Servers auf. Drücken Sie hierfür während des Boot des Servers die Taste F2.
- Rufen Sie das Menü *Server Mgmt* auf:

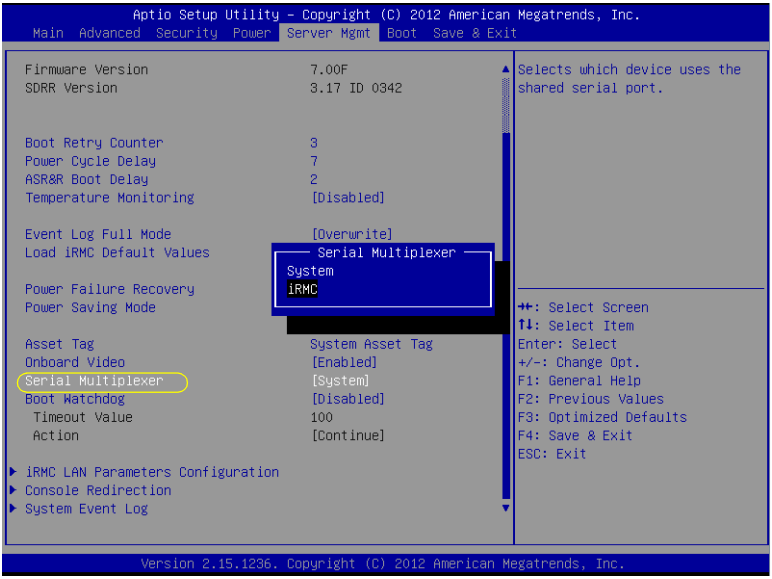



Bild 12: Menü Server Mgmt

- Konfigurieren Sie folgende Einstellungen:

*Serial Multiplexer*

Setzen Sie die Einstellung auf *iRMC*.

► Rufen Sie da Menü *Serial Port 1 Configuration* auf, um den seriellen Port zu konfigurieren:

*Advanced – Super IO Configuration – Serial Port 1 Configuration*:

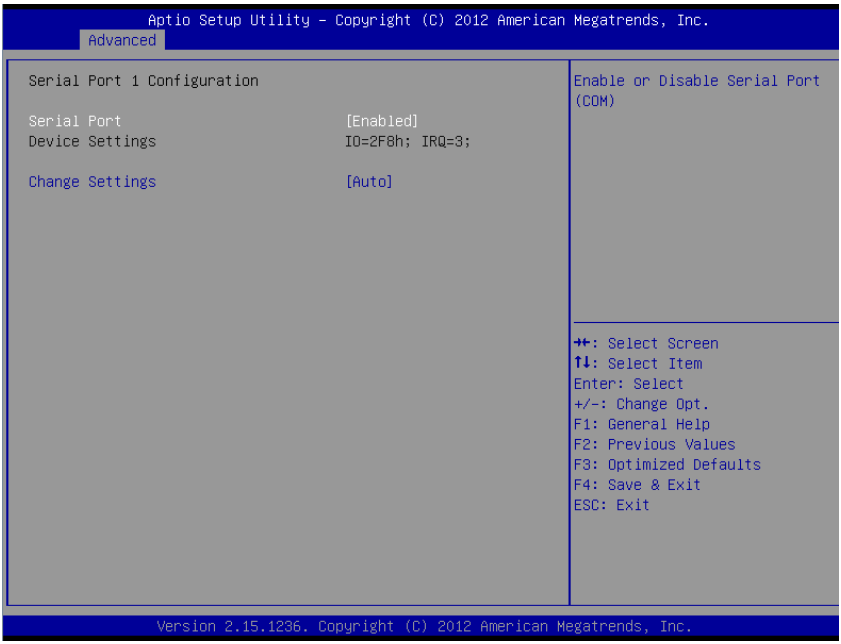



Bild 13: Menü Serial Port 1 Configuration

► Konfigurieren Sie folgende Einstellungen:

*Serial Port*

Setzen Sie die Einstellung auf *Enabled*.

*Device Settings*

Zeigt die Ein-/Ausgabe-Adresse und den Interrupt für den zugehörigen seriellen Port , z.B. IO=2F8h; IRQ=3.

Akzeptieren Sie den vorgeschlagenen Wert.

### UEFI Setup beenden

► Sichern Sie die Einstellungen und beenden Sie das UEFI Setup Utility.

► Fahren Sie fort mit Abschnitt "LAN-Schnittstelle testen" auf Seite 50.

### 3.3.2 Benutzeroberfläche Remote Manager (Serial) nutzen

Wenn Sie über eine Nullmodemkabel einen Rechner anschließen und auf diesem Rechner ein Terminalprogramm (VT100+) starten, können Sie auf die Terminal-Anwendung Remote Manager (Serial) zugreifen. Die Oberfläche des Remote Manager (Serial) ist identisch mit der Oberfläche des Remote Manager (siehe Kapitel "iRMC S4 über Telnet/SSH (Remote Manager)" auf Seite 387).

#### Voraussetzungen

Am verwalteten Server:

Die BIOS-Einstellung *Serial Multiplexer* muss auf *iRMC* konfiguriert sein (siehe Abschnitt "Die serielle Schnittstelle des iRMC S4 konfigurieren" auf Seite 56).

Terminalprogramm (VT100+):

Konfigurieren Sie für das Terminalprogramm folgende Port-Einstellungen:

*Bits per second*

Setzen Sie die Einstellung auf *38400*.

*Data bits*

Setzen Sie die Einstellung auf *8*.

*Parity*

Setzen Sie die Einstellung auf *None*.

*Stop-Bits*

Setzen Sie die Einstellung auf *1*.

*Flow Control*

Setzen Sie die Einstellung auf *None*.

# 3.4 iRMC S4 über die iRMC-Weboberfläche konfigurieren

► Starten Sie die iRMC-Weboberfläche (siehe Abschnitt "An der iRMC-Weboberfläche anmelden" auf Seite 134).

## 3.4.1 LAN-Parameter konfigurieren

► Wählen Sie im Navigationsbereich den Eintrag *Netzwerk Einstellungen* (siehe Abschnitt "Netzwerk Einstellungen - LAN-Parameter konfigurieren" auf Seite 268).

### LAN-Einstellungen konfigurieren

► Konfigurieren Sie die LAN-Einstellungen auf der Seite *Netzwerk Schnittstelle*. Für die erforderlichen Einstellungen siehe Abschnitt "Netzwerk Schnittstelle - Ethernet-Einstellungen des iRMC S4 konfigurieren" auf Seite 269.

### Ports und Netzwerk-Dienste konfigurieren

► Konfigurieren Sie die Ports und Netzwerk-Dienste in der Seite *Ports und Netzwerk Dienste*. Für die erforderlichen Einstellungen siehe Abschnitt "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 276.

### DHCP/DNS (Dynamic DNS) konfigurieren

► Konfigurieren Sie die DHCP- und DNS-Einstellungen in der Seite *DNS Konfiguration*. Für die erforderlichen Einstellungen siehe Abschnitt "DNS Konfiguration - DNS für den iRMC S4 konfigurieren" auf Seite 282.

## 3.4.2 Alarmbenachrichtigung (Alerting) konfigurieren

Die Seiten für die Konfiguration der Alarmbenachrichtigung sind im Navigationsbereich unter *Benachrichtigungen* zusammengefasst (siehe Abschnitt "Benachrichtigungen - Alarmbenachrichtigung konfigurieren" auf Seite 289).

### Weiterleitung von Alarmen über SNMP konfigurieren

- Klicken Sie im Navigationsbereich auf *SNMP Traps*. Die Seite *SNMP Traps* wird angezeigt.
- Konfigurieren Sie die Weiterleitung von SNMP Traps. Für die erforderlichen Einstellungen siehe Abschnitt "SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren" auf Seite 290.

### E-Mail-Benachrichtigung (Email Alerting) konfigurieren

- Klicken Sie im Navigationsbereich auf *Email*. Die Seite *E-Mail Benachrichtigung* wird angezeigt.
- Konfigurieren Sie die E-Mail-Benachrichtigung. Für die erforderlichen Einstellungen siehe Abschnitt "E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren" auf Seite 292.

## 3.4.3 Text-Konsolen-Umleitung konfigurieren

- Konfigurieren Sie die Umleitung der Text-Konsole im Fenster *BIOS Text Console*. Für die erforderlichen Einstellungen siehe Abschnitt "BIOS Text Konsole - Textkonsolen-Umleitung konfigurieren und starten" auf Seite 341.

# 4 Benutzerverwaltung für den iRMC S4

Die Benutzerverwaltung für den iRMC S4 verwendet zwei verschiedene Arten von Benutzerkennungen:

– **Lokale Benutzerkennungen** sind lokal im nicht-flüchtigen Speicher des iRMC S4 hinterlegt und werden über die Benutzerschnittstellen des iRMC S4 verwaltet.

– **Globale Benutzerkennungen** sind in der zentralen Datenhaltung eines Verzeichnisdienstes (Directory Service) hinterlegt und werden über die Schnittstellen dieses Verzeichnisdienstes verwaltet.

  Für die globale iRMC S4-Benutzerverwaltung werden zurzeit folgende Verzeichnisdienste unterstützt:

  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP
  – OpenDJ

Das vorliegende Kapitel informiert über folgende Themen:

– Konzept der Benutzerverwaltung für den iRMC S4
– Benutzerberechtigungen
– Lokale Benutzerverwaltung am iRMC S4

Detaillierte Informationen zur globalen Benutzerverwaltung für den iRMC S2/S3 mithilfe der einzelnen Verzeichnisdienste finden Sie im Handbuch „Benutzerverwaltung in ServerView“.

# 4.1 Konzept der Benutzerverwaltung für den iRMC S4

Die Benutzerverwaltung für den iRMC S4 unterstützt die parallele Verwaltung lokaler und globaler Benutzerkennungen.

Bei der Validierung der Authentifizierungsdaten (Benutzername, Passwort), die ein Benutzer beim Login an einer der iRMC S4-Schnittstellen eingibt, verfährt der iRMC S4 gemäß dem folgenden Ablauf (siehe auch Bild 14 auf Seite 64):

1. Der iRMC S4 gleicht den Benutzernamen und das Passwort mit den lokal gespeicherten Benutzerkennungen ab:
   - Bei erfolgreicher Authentifizierung des Benutzers durch den iRMC S4 (Benutzername und Passwort sind gültig) darf sich der Benutzer einloggen.
   - Andernfalls setzt der iRMC S4 die Prüfung mit Schritt 2. fort.
2. Der iRMC S4 authentifiziert sich selbst mit einem Benutzernamen und einer Passwort beim Directory Service via LDAP.

   Abhängig von seinen LDAP-Konfigurationseinstellungen, macht der iRMC S4 wie folgt weiter:

   - Wenn ServerView-spezifische LDAP-Gruppen mit Authentifizierungseinstellungen in der *SVS*-Struktur auf dem LDAP-Server verwendet werden, ermittelt der iRMC S4 die Benutzerberechtigungen über eine LDAP-Abfrage und überprüft, ob der Benutzer berechtigt ist, auf dem iRMC S4 zu arbeiten.

     Eigenschaften:

     – Keine Erweiterung der Directory Server-Struktur benötigt.
     – Rechte / Berechtigungen werden auf jeden iRMC S4 separat konfiguriert.
   - Wenn LDAP-Standardgruppen verwendet werden, für welche die Authentifizierungseinstellungen auf dem iRMC S4 lokal abgelegt sind, geht der iRMC S4 wie folgt vor:

     1. Der iRMC S4 verwendet eine LDAP-Abfrage um zu ermitteln, welcher Standard-LDAP-Gruppe auf dem Directory Server der Benutzer angehört..

2. Der iRMC S4 überprüft, ob eine Benutzergruppe mit diesem Namen auch lokal auf dem iRMC S4 konfiguriert ist. Wenn dies zutrifft, ermittelt der iRMC S4 die Benutzerberechtigungen mithilfe dieser lokalen Gruppe.

Eigenschaften:

– Erweiterung der Directory Server-Struktur benötigt.
– Rechte / Berechtigungen sind auf dem Directory Server zentral konfiguriert.

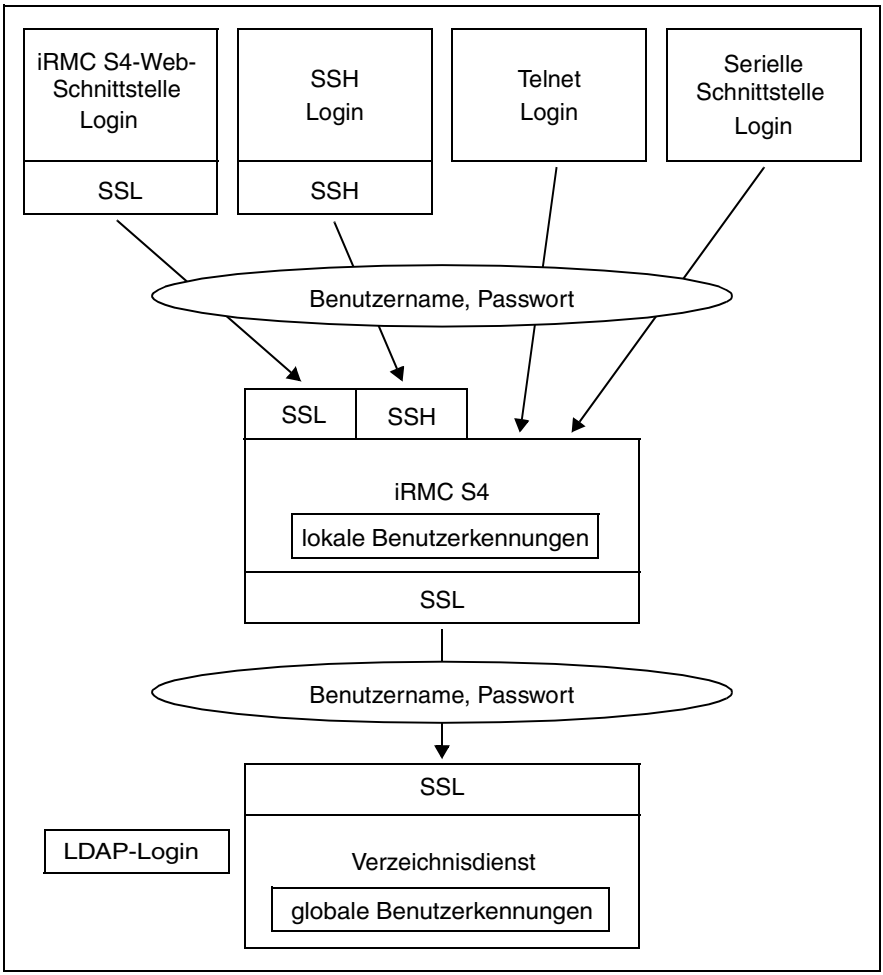



Bild 14: Login-Authentifizierung durch den iRMC S4

Die Nutzung von SSL für die LDAP-Verbindung zwischen dem iRMC S4 und dem Directory Service ist optional, wird jedoch empfohlen. Eine SSL-gesicherte LDAP-Verbindung zwischen iRMC S4 und Directory Service garantiert den sicheren Austausch der Daten, insbesondere auch von Benutzernamen und Passwort.

SSL-Login über die iRMC-Weboberfläche ist nur dann erforderlich, wenn LDAP aktiviert ist (Option (*LDAP aktiviert*, siehe Seite 314).

## 4.2 Benutzerberechtigungen

Der iRMC S4 unterscheidet zwei verschiedene Arten von Benutzerberechtigungen, die sich ergänzen:

– Kanal-spezifische Privilegien (via Zuordnung zu Kanal-spezifischen Berechtigungsgruppen)

– Berechtigungen zur Nutzung spezieller iRMC S4-Funktionen

Welche dieser Privilegien und Berechtigungen zur Nutzung der einzelnen iRMC S4-Funktionen erforderlich sind, ist beschrieben

  – für die iRMC-Weboberfläche auf Seite 136,

  – für den Remote Manager auf Seite 396.

**Kanal-spezifische Privilegien (Kanal-spezifische Berechtigungsgruppen)**

Der iRMC S4 ordnet jede Benutzerkennung einer der folgenden vier Kanal-spezifischen Berechtigungsgruppen zu:

– Benutzer
– Operator
– Administrator
– OEM

Da der iRMC S4 diese Berechtigungen Kanal-spezifisch erteilt, kann ein Benutzer verschiedene Rechte haben, je nachdem, ob er auf den iRMC S4 über die LAN-Schnittstelle oder über die serielle Schnittstelle zugreift.

Der Berechtigungsumfang nimmt beginnend bei *Benutzer* (niedrigste Berechtigungsstufe) über *Operator* und *Administrator*bis *OEM* (höchste Berechtigungsstufe) stetig zu.

Die Berechtigungsgruppen entsprechen dem IPMI Privilege Level. Bestimmte Rechte (z. B. für das Power Management) sind an diese Gruppen bzw. Privilege Level gebunden.

Um den iRMC S4 zur Serverliste des ServerView Operations Manager hinzuzufügen, werden die LAN-Privilegien Administrator oder OEM benötigt (siehe Handbuch "ServerView Operations Manager").

### Berechtigungen zur Nutzung spezieller iRMC S4-Funktionen

Zusätzlich zu den Kanal-spezifischen Berechtigungen können Sie einem Benutzer individuell folgende Berechtigungen erteilen:

- **Configure User Accounts**
  Berechtigung zum Konfigurieren von lokalen Benutzerkennungen
- **Configure iRMC S4 Settings**
  Berechtigung zum Konfigurieren von iRMC S4-Einstellungen.
- **Video Redirection Enabled**
  Berechtigung zur Nutzung der Grafischen Konsolen-Umleitung (Advanced Video Redirection (AVR)) im “Nur Lesen”- und “Volle Kontrolle”-Modus
- **Remote Storage Enabled**
  Berechtigung zur Nutzung der Virtual Media-Funktionalität

### Vorkonfigurierte Benutzerkennung

Die Firmware des iRMC S4 stellt eine Standard-Administratorkennung für den iRMC S4 zur Verfügung, die sämtliche Berechtigungen besitzt:

*Administratorkennung*: admin

*Passwort*: admin

Für Administratorkennung und Kennwort wird bei lokalen Benutzern zwischen Groß- und Kleinschreibung unterschieden.

Es wird dringend empfohlen, nach der Anmeldung möglichst bald eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Kennwort der Kennung zu ändern (siehe Abschnitt "Benutzerverwaltung" auf Seite 299).

# 4.3 Lokale Benutzerverwaltung für den iRMC S4

Der iRMC S4 verfügt über eine eigene lokale Benutzerverwaltung. Es können bis zu 16 Benutzer mit Kennwörtern konfiguriert und je nach Gruppenzugehörigkeit mit unterschiedlichen Rechten ausgestattet werden. Die Benutzerkennungen werden im lokalen, nicht-flüchtigen Speicher des iRMC S4 abgelegt.

Für die Benutzerverwaltung am iRMC S4 stehen Ihnen folgende Möglichkeiten zur Verfügung:

– Benutzerverwaltung über die Weboberfläche

– Benutzerverwaltung über den Server Configuration Manager

## 4.3.1 Lokale Benutzerverwaltung über die iRMC S4-Weboberfläche

Die Benutzerverwaltung am iRMC S4 erfordert die Berechtigung *Benutzer konfigurieren erlaubt*.

An der Weboberfläche können Sie sich die Liste der konfigurierten Benutzer anzeigen lassen. Außerdem können Sie neue Benutzer konfigurieren, die Konfiguration bereits existierender Benutzer ändern sowie Benutzer aus der Liste entfernen.

► Starten Sie die iRMC S4-Weboberfläche (siehe Abschnitt "An der iRMC-Weboberfläche anmelden" auf Seite 134).

### Liste der konfigurierten Benutzer anzeigen

► Klicken Sie im Navigationsbereich auf den die Funktion *Benutzerverwaltung - iRMC S4 Benutzer*.

Die Seite *Benutzer Verwaltung* mit der Liste der konfigurierten Benutzer öffnet sich (sieheSeite 300). Dort können Sie Benutzer löschen sowie die Seite für die Konfiguration neuer Benutzer aufrufen.
Die Beschreibung zu dieser Seite finden Sie im Abschnitt "Benutzerverwaltung" auf Seite 299.

#### Neuen Benutzer konfigurieren

- Klicken Sie in der Seite *Benutzer Verwaltung* auf die Schaltfläche *Neuer Benutzer*.

  Die Seite *Neuen Benutzer konfigurieren* öffnet sich. In dieser Seite können Sie die Grundeinstellungen des neuen Benutzers konfigurieren. Die Beschreibung zu dieser Seite finden Sie im Abschnitt "Neuen Benutzer konfigurieren" auf Seite 301.

#### Konfiguration eines Benutzers ändern

- Klicken Sie in der Seite *Benutzer Verwaltung* auf den Namen des Benutzers, dessen Konfigurationsparameter Sie ändern wollen.

  Die Seite *Benutzer '<name>' Konfiguration* öffnet sich mit den Einstellungen des ausgewählten Benutzers. Dort können Sie die Konfigurationsparameter des neuen Benutzers ändern. Die Beschreibung zu dieser Seite finden Sie im Abschnitt "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 302.

#### Benutzer löschen

- Klicken Sie in der Seite *Benutzer Verwaltung* auf die Schaltfläche *Löschen*, die sich in der Zeile des zu löschenden Benutzers befindet.

### 4.3.2 Lokale Benutzerverwaltung über den Server Configuration Manager

**Voraussetzung:**

Auf dem verwalteten Server sind die aktuellen ServerView Agents installiert.

Die Benutzerverwaltung am iRMC S4 erfordert die Berechtigung *Benutzer konfigurieren erlaubt*.

Die Benutzerverwaltung mit dem Server Configuration Manager entspricht weitgehend der Benutzerverwaltung via iRMC S4-Weboberfläche.

Im Kapitel "iRMC S4 via Server Configuration Manager konfigurieren" auf Seite 413 ist beschrieben, wie Sie den Server Configuration Manager starten.

Näheres zu den einzelnen Dialogen des Server Configuration Managers finden Sie in der Online-Hilfe des Server Configuration Managers.

### 4.3.3 SSHv2 Public Key-Authentifizierung für lokale iRMC S4-Benutzer

Neben der Authentisierung mit Benutzername und Passwort unterstützt der iRMC S4 für lokale Benutzer zusätzlich die SSHv2-basierte Public Key-Authentisierung mithilfe von Paaren aus öffentlichem und privatem Schlüssel. Für die SSHv2 Public Key-Authentifizierung wird der öffentliche SSHv2-Schlüssel eines iRMC S4-Benutzers auf den iRMC S4 geladen, während der iRMC S4-Benutzer seinen privaten Schlüssel z.B. über das Programm *PuTTY* oder das OpenSSH Client-Programm *ssh* verwendet.

Der iRMC S4 unterstützt die folgenden Typen öffentlicher Schlüssel:

– SSH DSS (mindestens erforderlich)
– SSH RSA (empfohlen)

Die öffentlichen SSHv2-Schlüssel (SSHv2 Public Keys), die Sie auf den iRMC S4 laden, können wahlweise in einem Format gemäß RFC4716 oder im OpenSSH-Format vorliegen (siehe Seite 81).

#### Public Key-Authentifizierung

In groben Zügen stellt sich Public Key-Authentifizierung eines Benutzers am iRMC S4 wie folgt dar:

Der Benutzer, der sich am iRMC S4 anmelden will, erzeugt das Schlüsselpaar:

– Der private Schlüssel bleibt lesegeschützt auf dem Computer des Benutzers.

– Den öffentlichen Schlüssel lädt der Benutzer (oder der Administrator) auf den iRMC S4.

Bei entsprechender Konfiguration kann sich der Benutzer nun ohne Passwort und sehr sicher an diesem iRMC S4 anmelden. Der Benutzer ist lediglich für die Geheimhaltung seines privaten Schlüssels verantwortlich.

Die folgenden Schritte sind notwendig, um eine Authentfizierung mit privatem Schlüssel einzurichten. Die Schritte sind in den nächsten Abschnitten beschrieben:

1. Öffentlichen und privaten SSHv2-Schlüssel mit dem Programm *PuTTYgen* oder *ssh-keygen* erzeugen und in separate Dateien sichern (siehe Seite 70).
2. Öffentlichen SSHv2-Schlüssel aus Datei auf den iRMC S4 laden (siehe Seite 74).

3. Das Programm *PuTTY* bzw. *ssh* für den SSHv2-Zugriff auf den iRMC S4 konfigurieren (siehe Seite 76).

#### 4.3.3.1 Öffentlichen und privaten SSHv2-Schlüssel erzeugen

Den öffentlichen und den privatenSSHv2-Schlüssel erzeugen Sie wahlweise

– mit dem Programm *PuTTYgen* oder

– mit dem OpenSSH-Client-Programm *ssh-keygen*.

**Öffentlichen und privaten SSHv2-Schlüssel mit PuTTYgen erzeugen**

Gehen Sie wie folgt vor:

► Starten Sie *PuTTYgen* auf Ihrem Windows-Rechner

Nach dem Start meldet sich *PuTTYgen* mit dem folgenden Fenster:

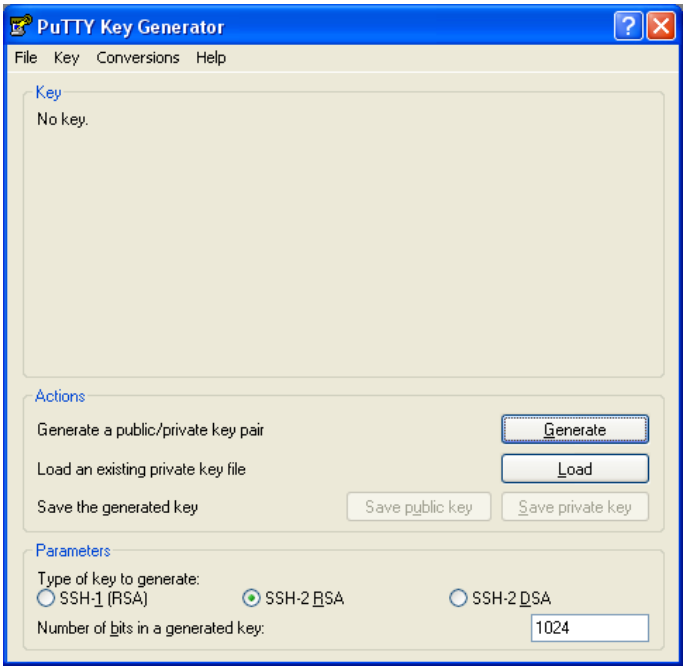



Bild 15: PuTTYgen: Neuen privaten und öffentlichen SSHv2-Schlüssel erzeugen

► Wählen Sie unter *Parameters* den Schlüsseltyp *SSH-2RSA* und klicken Sie auf *Generate*, um die Schlüsselgenerierung zu starten.

Danach wird unter *Key* der Generierungsfortschritt angezeigt (siehe Bild 16 auf Seite 71).

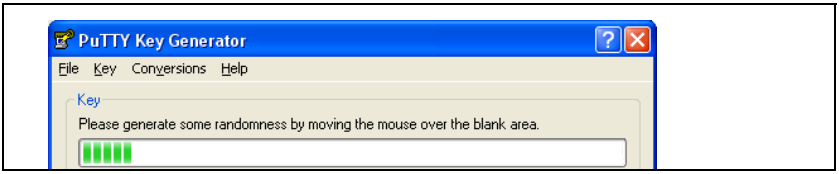

PuTTY Key Generator
File Key Conversions Help
Key
Please generate some randomness by moving the mouse over the blank area.

Bild 16: PuTTYgen: Neues Schlüsselpaar erzeugen (Fortschrittsanzeige).

► Bewegen Sie den Mauszeiger über die freie Fläche der Fortschrittsanzeige, um die Zufälligkeit der generierten Schlüssel zu erhöhen.

Nach Abschluss der Schlüsselgenerierung zeigt *PuTTYgen* Schlüssel und Fingerprint des öffentlichen SSHv2-Schlüssels an:

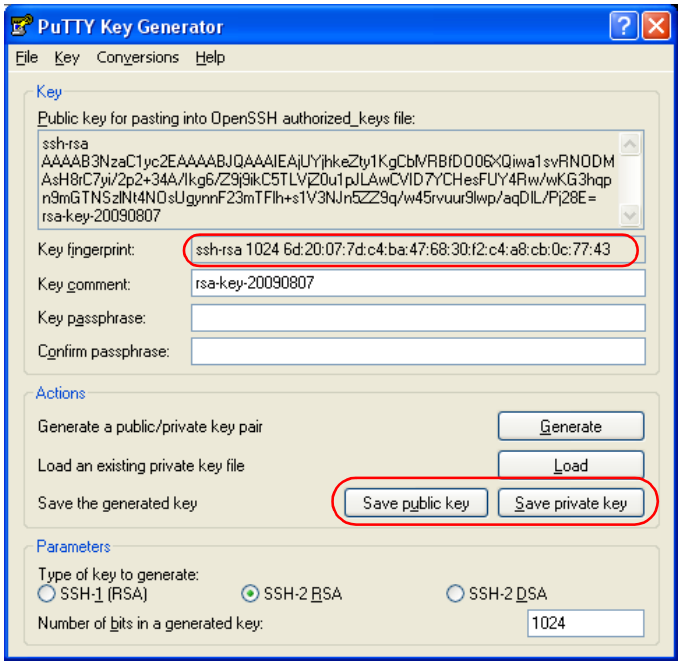



Bild 17: PuTTYgen: Neuen privaten SSHv2-Schlüssel erzeugen (Fortschrittsanzeige).

- Klicken Sie auf *Save public key*, um den öffentlichen SSHv2-Schlüssel in eine Datei zu speichern. Aus dieser Datei können Sie den öffentlichen Schlüssel auf den iRMC S4 hochladen (siehe Seite 74).
- Klicken Sie auf *Save private key*, um den privaten SSHv2-Schlüssel für die Verwendung mit *PuTTY* (siehe Seite 76) in eine Datei zu speichern.

### Öffentlichen und privaten SSHv2-Schlüssel mit ssh-keygen erzeugen

Sofern OpenSSH in der von Ihnen verwendeten Linux-Distribution nicht bereits installiert ist, können Sie OpenSSH von *http://www.openssh.org* beziehen.

Die ausführliche Beschreibung der Operanden finden Sie auf den Man Pages von OpenSSH unter *http://www.openssh.org/manual.html*

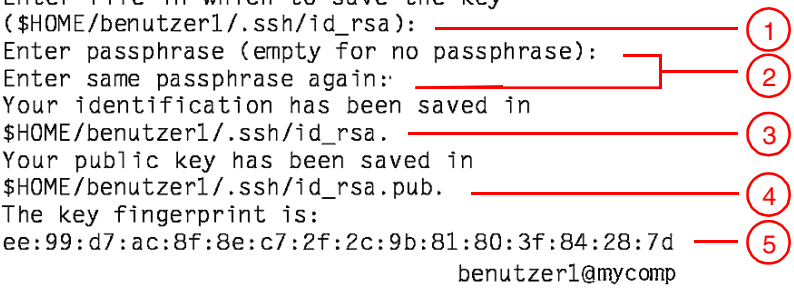
Gehen Sie wie folgt vor:

- Rufen Sie *ssh-keygen* für die Generierung eines RSA-Schlüsselpaars auf:

  ```
  ssh-keygen -t rsa
  ```

  *ssh-keygen* protokolliert den Ablauf der Schlüsselgenerierung. Dabei fragt *ssh-keygen* nach dem Dateinamen, unter dem der private Schlüssel abgespeichert werden soll, sowie nach einer Passphrase für den privaten Schlüssel. Als Ergebnis speichert *ssh-keygen* privaten und öffentlichen SSHv2-Schlüssel in separaten Dateien ab und zeigt den Fingerprint des öffentlichen Schlüssels an.

  *Beispiel: RSA-Schlüsselpaar mit ssh -keygen generieren*



Erläuterung:

1. *ssh-keygen* fragt nach dem Dateinamen, unter dem der private SSHv2-Schlüssel abgespeichert werden soll. Wenn Sie ohne Eingabe eines Dateinamens mit Enter bestätigen, verwendet *ssh-keygen* den Standard-Dateinamen *id_rsa*.
2. *ssh-keygen* fordert Sie auf, eine Passphrase (inklusive Bestätigung) zur Verschlüsselung des privaten Schlüssels einzugeben. Wenn Sie ohne Eingabe einer Passphrase mit Enter bestätigen, verwendet *ssh-keygen* keine Passphrase.
3. *ssh-keygen* informiert, dass der neu generierte private SSHv2-Schlüssel in der Datei */.ssh/id_rsa* gespeichert wurde.
4. *ssh-keygen* informiert, dass der neu generierte öffentliche SSHv2-Schlüssel in der */.ssh/id_rsa.pub* gespeichert wurde.
5. *ssh-keygen* zeigt Fingerprint des öffentlichen SSHv2-Schlüssels sowie die lokale Benutzkennung, zu der der öffentliche Schlüssel gehört.

### 4.3.3.2 Öffentlichen SSHv2-Schlüssel aus Datei auf den iRMC S4 laden.

Gehen Sie wie folgt vor:

► Öffnen Sie in der iRMC S4 Weboberfläche über die Seite *iRMC S4 User Management* die Detailansicht für den gewünschten Benutzer (hier *user3*) :

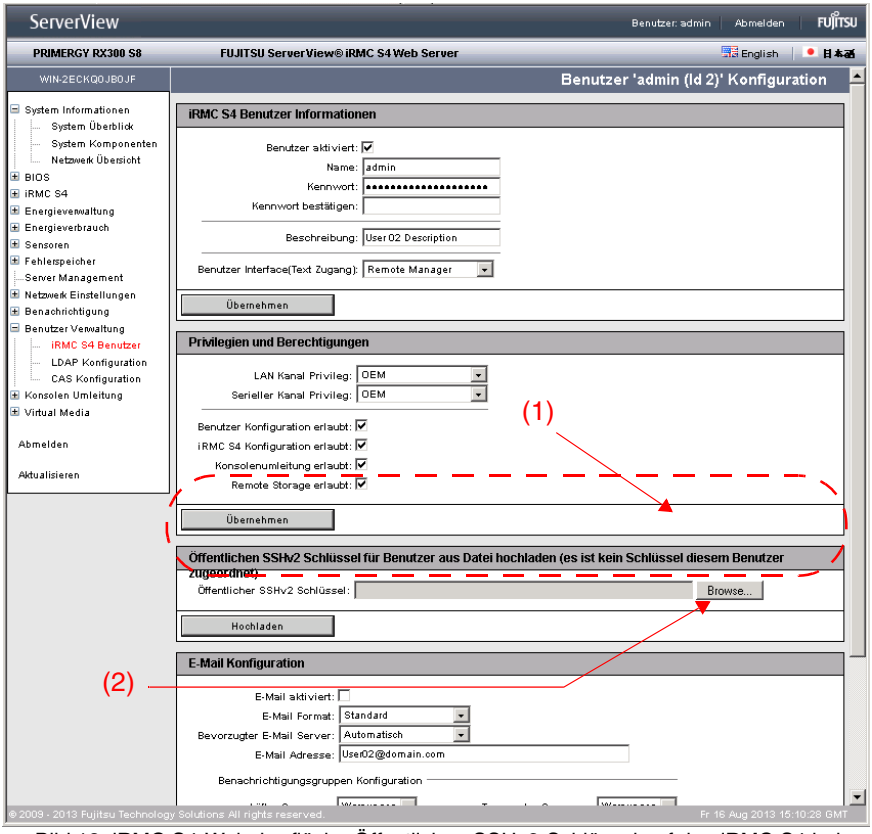



Bild 18: iRMC S4-Weboberfläche Öffentlichen SSHv2-Schlüssel auf den iRMC S4 laden

► Klicken Sie in der Gruppe *Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen* auf *Durchsuchen* (1), und navigieren Sie zu der Datei, die den gewünschten öffentlichen Schlüssel enthält (2).

► Klicken Sie auf *Hochladen*, um den öffentlichen Schlüssel auf den iRMC S4 zu laden.

Nach erfolgreichem Hochladen zeigt der iRMC S4 den Key Fingerprint in der Gruppe *Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen* an:

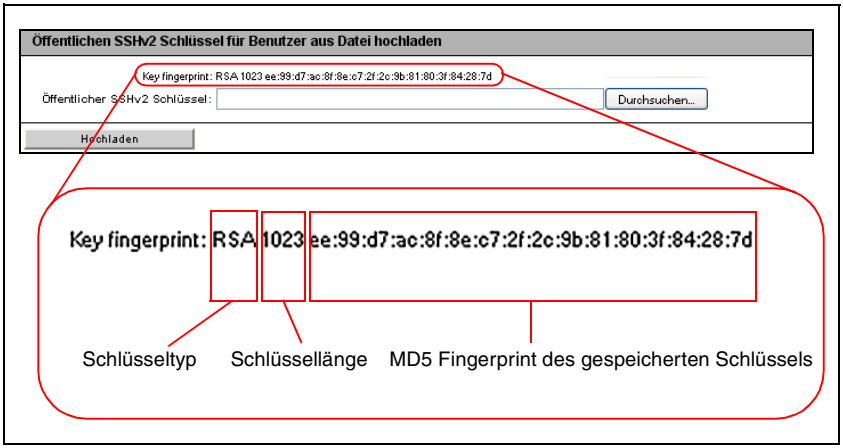



Bild 19: Anzeige des Key fingerprint

Vergewissern Sie sich aus Sicherheitsgründen, dass der hier angezeigte Fingerprint mit dem in *PuTTYgen* (siehe Bild 17 auf Seite 71) unter *Key fingerprint* angezeigten Fingerprint übereinstimmt.

#### 4.3.3.3 PuTTY und OpenSSH Client für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren

### PuTTY für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren

Mithilfe des Programms *PuTTY* können eine Public Key-authentifizierte Verbindung zum iRMC S4 herstellen und sich dort wahlweise unter Ihrem Benutzernamen oder via Auto-Login anmelden. Dabei wickelt *PuTTY* das Authentifizierungsprotokoll automatisch auf Basis des zuvor erzeugten Paars aus privatem und öffentlichem SSHv2-Schlüssel ab.

Gehen Sie wie folgt vor:

- Starten Sie *PuTTY* auf Ihrem Windows Computer.

  Nach dem Start meldet sich *PuTTY* mit dem folgenden Fenster:

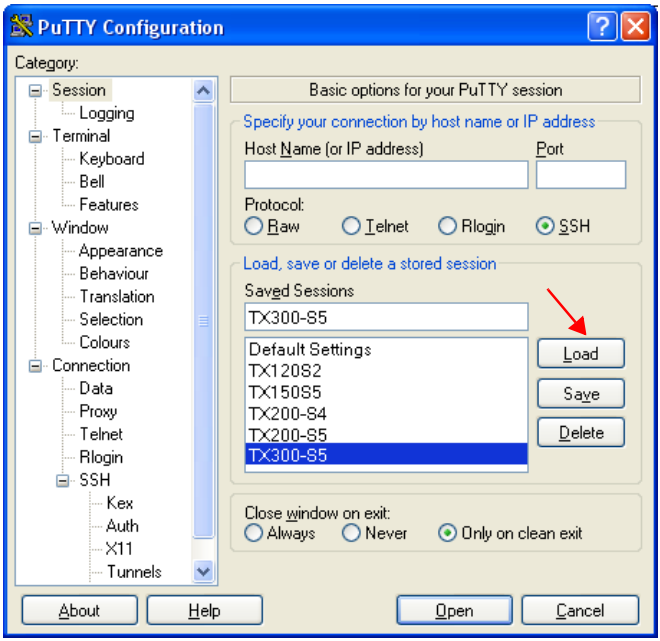



Bild 20: PuTTY: SSH-Sitzung auswählen und laden

- Wählen Sie eine gespeicherte SSH-Sitzung oder erzeugen Sie eine neue SSH-Sitzung für den iRMC S4, mit dem Sie den öffentlichen SSHv2-Schlüssel verwenden wollen.

► Klicken Sie auf *Load*, um die gewählte SSH-Sitzung zu laden.

Das folgende Fenster wird angezeigt:

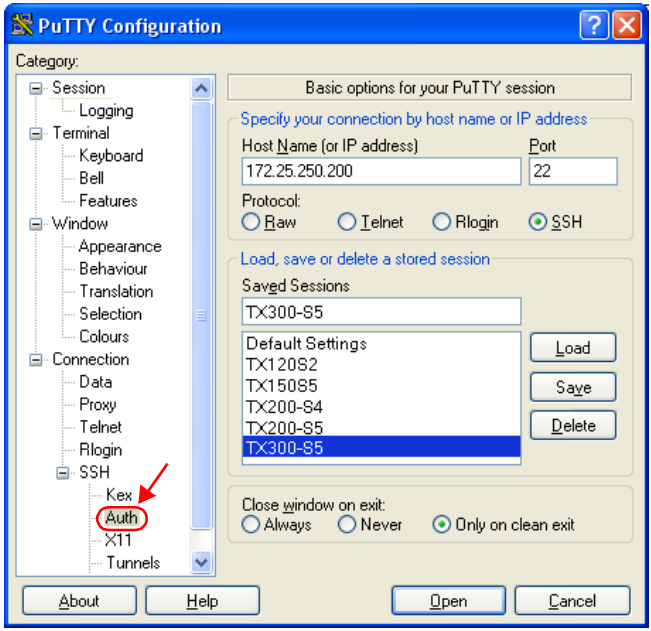



Bild 21: PuTTY: SSH-Sitzung geladen

► Wählen Sie *SSH - Auth*, um die Optionen für die SSH-Authentifizierung zu konfigurieren.

Das folgende Fenster wird angezeigt (siehe Bild 22 auf Seite 78):

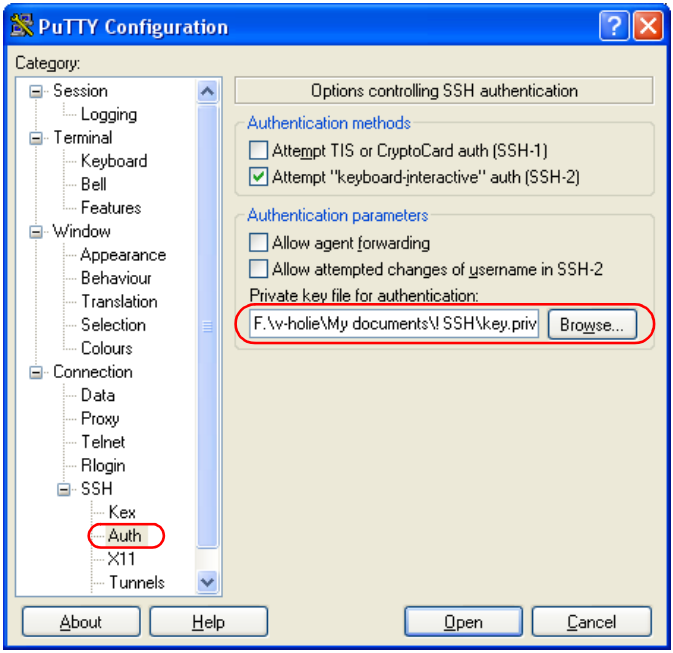



Bild 22: Optionen für die SSH-Authentifizierung konfigurieren

► Wählen Sie die Datei, die den privaten Schlüssel enthält, den Sie mit dem iRMC S4 verwenden wollen.

**Beachten Sie:**
An dieser Stelle wird der private Schlüssel (siehe Seite 71) benötigt und **nicht** der öffentliche Schlüssel, den Sie auf den iRMC S4 geladen haben.

Zusätzlich können Sie unter *Connection - Data* eine Benutzernamen für das Auto-Login am iRMC S4 angeben:

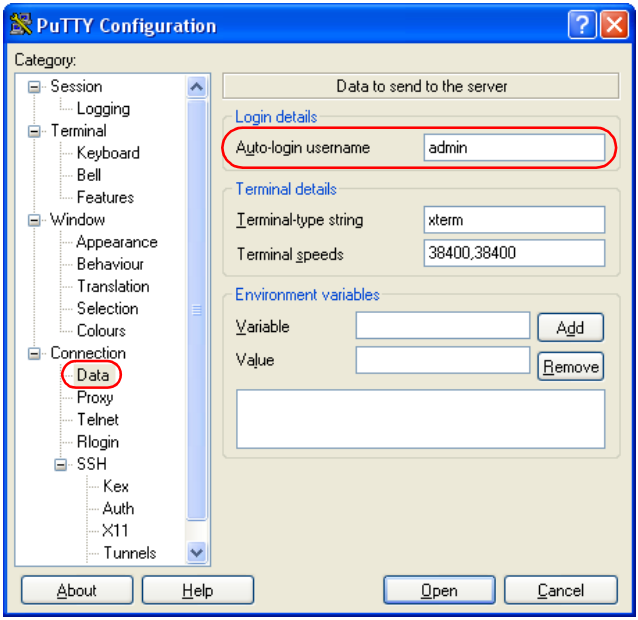



Bild 23: PuTTY: Benutzernamen für Auto-Login am iRMC S4 angeben.

### OpenSSH Client-Programm ssh für die Nutzung des öffentlichen SSHv2-Schlüssels konfigurieren

Mithilfe des OpenSSH Client-Programms *ssh* stellen Sie eine SSHv2-gesicherte Verbindung zum iRMC S4 her. Dabei können Sie sich wahlweise unter Ihrer aktuellen lokalen Benutzerkennung oder einer anderen Benutzerkennung anmelden.

Voraussetzung ist, dass die betreffende Benutzerkennung als lokale Benutzerkennung am iRMC S4 konfiguriert ist und der zugehörige öffentliche SSHv2-Schlüssel auf den iRMC S4 geladen wurde.

*ssh* liest seine Konfigurationsoptionen der Reihe nach aus folgenden Quellen:

1. Kommandozeilen-Argumente, die Sie beim Aufruf von *ssh* angeben.
2. benutzerspezifische Konfigurationsdatei (*$HOME/.ssh/config*)

Obwohl diese Datei in der Regel keine sicherheitskritischen Informationen enthält, sollte Lese-/Schreibberechtigung lediglich für den Eigentümer bestehen. Allen anderen Benutzern sollte der Zugriff verweigert werden.

3. systemweite Konfigurationsdatei (*/etc/ssh/ssh_config*)

   Diese Datei enthält Default-Werte für Konfigurationsparameter,

   – wenn keine benutzerspezifische Konfigurationsdatei existiert oder

   – wenn die entsprechenden Parameter nicht in der benutzerspezifischen Konfigurationsdateispezifiziert sind.

Für jede Option gilt der zuerst gefundene Wert.

Ausführliche Informationen zu Konfiguration und Operanden von *ssh* finden Sie auf den Man Pages von OpenSSH unter

*http://www.openssh.org/manual.html*

Gehen Sie wie folgt vor:

► Starten Sie *ssh* um sich SSHv2-authentifiziert am iRMC S4 anzumelden:

```
ssh -l [<benutzer>] <iRMC_S4>
```

oder

```
ssh -l [<benutzer>@] <iRMC_S4>
```

<benutzer>
: Benutzername, unter dem Sie sich am iRMC S4 anmelden wollen. Wenn Sie <benutzer> nicht angeben, verwendet *ssh* für die Anmeldung am iRMC S4 den Benutzernamen, unter dem Sie an Ihrem lokalen Computer angemeldet sind.

<iRMC_S4>
: iRMC S4-Name oder IP-Adresse des iRMC S4, an dem Sie sich anmelden wollen.

*Beispiel: SSHv2-authentifizierte Anmeldung am iRMC S4*

Für den folgenden *ssh*-Aufruf wird vorausgesetzt, dass mit *ssh-keygen* ein Paar aus privatem und öffentlichem RSA-Schlüssel analog dem "Beispiel: RSA-Schlüsselpaar mit ssh -keygen generieren" auf Seite 72 erzeugt wurde und dass der öffentliche Schlüssel *Benutzer1/.ssh/id_rsa.pub* auf für einen iRMC S4-Benutzer *user4* den iRMC S4 geladen wurde (siehe Seite 74).

Sie können sich dann von Ihrem lokalen Computer unter *$HOME/Benutzer1* wie folgt am iRMC S4 „RX300_S82-iRMC“ unter der Benutzerkennung *user4* anmelden:

```
ssh user4@RX300_S82-iRMC
```

#### 4.3.3.4 Beispiel: Öffentlicher SSHv2-Schlüssel

Im Folgenden ist derselbe öffentliche SSHv2-Schlüssel sowohl im Format gemäß RFC4716 als auch im OpenSSH-Format abgedruckt.

**Öffentlicher SSHv2 Schlüssel im Format gemäß RFC4716**

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20090401"
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGsfc+F
pGJ2iw==
---- END SSH2 PUBLIC KEY ----
```

**Öffentlicher SSHv2 Schlüssel im OpenSSH-Format**

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAIBScBsgP9B74qNa9+w8Ccv3kDVVu2boKCGLv4hx
v6+AUFrF6sYdGey1QQ7MkwSeax3NmoZBkvkR9hNfZSqxkPCkd//LyUil9US5/9Ar
JxjlhXUzlPPVzuBtPaRB7+bISTJVMUorNwrcN48b6AAoYBhKC4AOtOP1OGwsfc+F
pGJ2iw== rsa-key-20090401
```

# 5 Advanced Video Redirection (AVR)

Die Nutzung der Funktion „Grafische Konsolen Umleitung (Advanced Video Redirection“) setzt einen gültigen KVM-Lizenzschlüssel (License Key) voraus.

Java Caching **darf nicht** ausgeschaltet sein. Andernfalls kann AVR nicht gestartet werden. (Java Caching ist standardmäßig eingeschaltet).

Mit der Grafische Konsolen-Umleitung (Advanced Video Redirection, AVR) können Sie von Ihrem Remote-Arbeitsplatz aus Tastatur und Maus des verwalteten Servers kontrollieren und sich die aktuellen grafischen Ausgaben sowie die Text-Ausgaben des verwalteten Servers anzeigen lassen.

Über das Java-Applet der AVR können Sie die Funktion „Virtual Media“ nutzen (siehe Kapitel "Virtuelle Medien Wizard" auf Seite 123).

Das vorliegende Kapitel informiert über folgende Themen:

- Einstellungen für die AVR prüfen
- AVR über ein Java-Applet verwenden
- AVR über HTML5 verwenden

# 5.1 Voraussetzung: Die Einstellungen für die AVR überprüfen

Bevor Sie AVR nutzen, prüfen Sie folgende wichtige Einstellungen:

**Einstellungen für den Grafikmodus am verwalteten Server**

AVR unterstützt die folgenden Grafikmodi:

| Auflösung | Wiederholungsraten [in Hz] | Maximale Farbtiefe [bit] |
|---|---|---|
| 640 x 480 (VGA) | 60; 75; 85 | 32 |
| 800 x 600 (SVGA) | 56; 60; 72; 75; 85 | 32 |
| 1024 x 768 (XGA) | 60; 70; 75; 85 | 32 |
| 1152 x 864 | 60; 70; 75 | 32 |
| 1280 x 1024 (UXGA) | 60; 70; 75; 85 | 16 |
| 1280 x 1024 (UXGA) | 60 | 24 |
| 1600 x 1200 (UXGA) | 60; 65 | 16 |
| 1680 x 1050 | 60 | 16 |
| 1920 x 1080 | 60 | 16 |
| 1920 x 1200 | 60 | 16 |

Tabelle 3: Unterstützte Einstellungen für die Bildanzeige

Es werden ausschließlich VESA-konforme Grafikmodi unterstützt.

### Unterstützter Text-Modus

Der iRMC S4 unterstützt die folgenden gebräuchlichen Text-Modi:

- 40 x 25
- 80 x 25
- 80 x 43
- 80 x 50

Für Informationen zu den Einstellungen für die Bildanzeige siehe die Hilfe zum Betriebssystem.

### Tastatur-Einstellungen

Wenn die Spracheinstellungen der Tastatur auf der Remote-Workstation sich von denen auf dem verwalteten Server unterscheiden, müssen die Spracheinstellungen der AVR-Tastatur mit denen des verwalteten Servers übereinstimmen.

Eine Zuordnung ist zwischen den folgenden Sprachen möglich:

- *Auto Detect* (Standardwert)
- *Englisch (US)*
- *Englisch (UK)*
- *Französisch*
- *Französisch (Belgien)*
- *Deutsch (Deutschland)*
- *Deutsch (Schweiz)*
- *Japanisch*
- *Spanisch*
- *Italienisch*
- *Dänisch*
- *Finnisch*
- *Norwegisch (Norwegen)*
- *Portugiesisch (Portugal)*
- *Schwedish*
- *Niederländisch (Niederlande)*
- *Niederländisch (Belgien)*
- *Türkisch - F*
- *Türkisch - Q*

Es können nicht alle Tasten zugeordnet werden. Wenn eine Taste nicht funktioniert, verwenden Sie das SoftKeyboard (siehe Seite 94).

## 5.2 AVR über ein Java-Applet verwenden

Zum Starten der AVR haben Sie folgende Möglichkeiten:

- Klicken Sie auf die Schaltfläche *Video Umleitung starten (Java Web Start)* auf der Seite *Grafische Konsolen Umleitung (AVR)* der iRMC S4-Weboberfläche (siehe Seite 346)

  oder, wenn angezeigt,

- Klicken Sie auf den Link *Video Umleitung (JWS)* in der Baumstruktur der iRMC S4-Weboberfläche.

  Es wird dann das Fenster *Advanced Video Redirection* (AVR-Fenster) geöffnet, das die Bildschirmausgabe am verwalteten Server darstellt.

## 5.2.1 AVR-Fenster

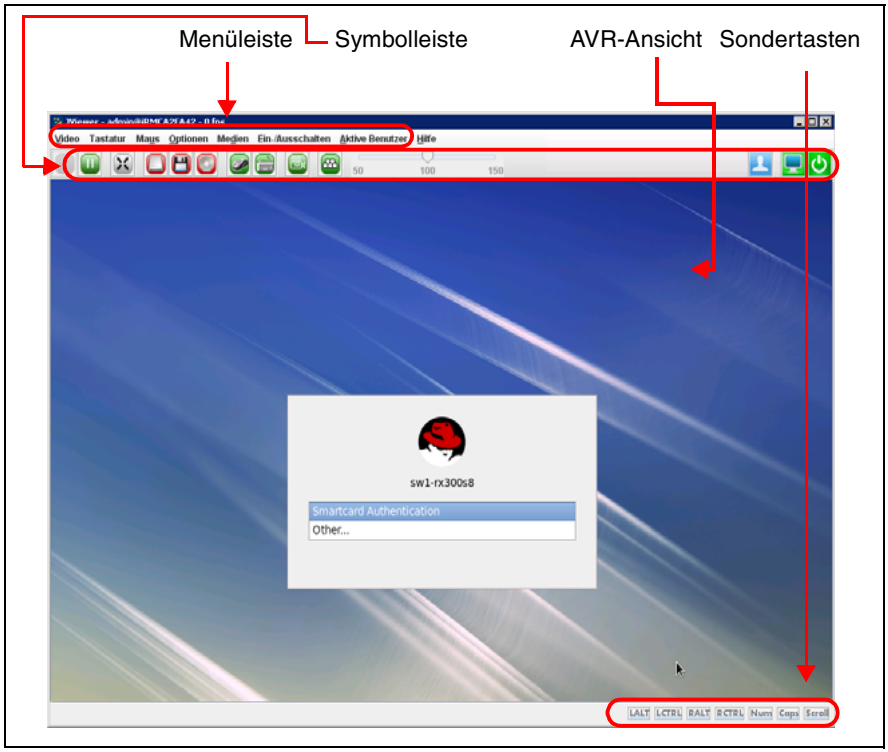



Bild 24: Fenster Video Umleitung (AVR-Fenster)

Das AVR-Fenster enthält auch die folgenden Elemente:

- Die AVR-Menüleiste bietet Zugriff auf die individuellen AVR-Menüs (siehe Seite 96).
- Mit der AVR-Symbolleiste können Sie direkt auf eine Vielzahl von AVR-Funktionen zugreifen, zum Beispiel Ihre AVR-Sitzung stoppen/wiederaufnehmen, die Funktion *Virtuelle Medien* verwenden, Ihre AVS-Sitzung aufzeichnen und Hotkeys verwenden (siehe Seite 93).
- Mit der Zoom-Symbolleiste können Sie die AVR-Ansicht stufenlos vergrößern oder verkleinern (siehe Seite 118).

- Mithilfe der integrierten Sondertasten rechts unten im AVR-Fenster können Sie Windows-Tasten oder spezielle Tastenkombinationen nutzen, die bei Eingabe über Ihre Tastatur nicht via AVR übertragen werden können (siehe Seite 93).

### 5.2.2 Geringe Bandbreite verwenden

Für den Fall, dass nur eine eingeschränkte Datentransfer-Rate verfügbar ist, können Sie für die Dauer Ihrer aktuellen AVR-Sitzung eine geringere Bandbreite (Bits pro Pixel, BPP) hinsichtlich der Farbtiefe konfigurieren.

### 5.2.3 Parallele AVR-Sitzungen

AVR kann von zwei Benutzer-Sitzungen gleichzeitig verwendet werden. Die zuerst gestartete AVR-Sitzung befindet sich anfänglich im *Vollzugriff*-Modus und hat die vollständige Kontrolle über den Server.

#### Zweite AVR-Sitzung starten, während die erste Sitzung noch aktiv ist

Für Situationen, in denen eine zweite AVR-Sitzung gestartet wird, während die vorherige erste AVR-Sitzung noch aktiv ist und sich im *Vollzugriff*-Modus befindet, erhalten Sie nachfolgend weitere Anweisungen.

– Im AVR-Fenster der Sitzung 1 wird das Dialogfenster *Berechtigungen freigeben für virtuelle Konsole* geöffnet, in dem ein Countdown von 30 Sekunden abläuft:

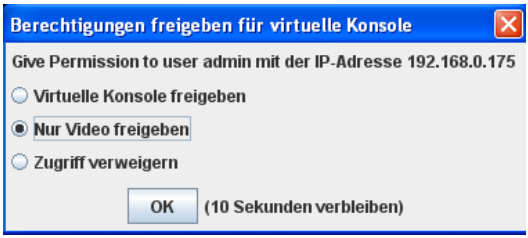



Bild 25: Dialogfenster Berechtigungen freigeben für virtuelle Konsole - Give Permission to ...

*Virtuelle Konsole freigeben*
: Sitzung 2 wechselt in den *Vollzugriff*-Modus Sitzung 1 wechselt in den *Teilzugriff (nur Video)*-Modus.

Virtuelle Medienverbindungen der Sitzung 1 werden gelöscht.

*Nur Video freigeben*

Sitzung 2 wechselt in den *Teilzugriff (nur Video)*-Modus. In diesem Modus können Sie die Tastatur- und Mausvorgänge des Servers nur passiv beobachten. Nur die *Video*- und *Aktive Benutzer*-Funktionen können verwendet werden.

Sitzung 1 bleibt weiterhin im *Vollzugriff*-Modus.

*Zugriff verweigern*

Sitzung 2 wird der Zugriff verwehrt und daraufhin geschlossen. Sitzung 1 bleibt weiterhin im *Vollzugriff*-Modus.

Wenn der Zähler abläuft, bevor Sitzung 1 mit *OK* bestätigt wurde, wechselt Sitzung 2 in den *Vollzugriff*-Modus. Sitzung 1 wechselt in den *Teilzugriff (nur Video)*-Modus.

### "Vollzugriff" anfordern wenn zwei AVR-Sitzungen gerade aktiv sind

Wenn zwei AVR-Sitzungen gerade aktiv sind und Sitzung 1 diejenige ist, die sich nicht im *Vollzugriff*-Modus befindet, kann Benutzer 1 der Sitzung 1 *Vollzugriff* anfordern durch Klicken auf *Volle Berechtigung anfordern* im Menü *Optionen* im AVR-Fenster (siehe Seite 112).

In diesem Fall wird Benutzer 2 der gleichzeitig laufenden AVR-Sitzung 2 aufgefordert, der AVR-Sitzung 1 *Vollzugriff:* zu erteilen.

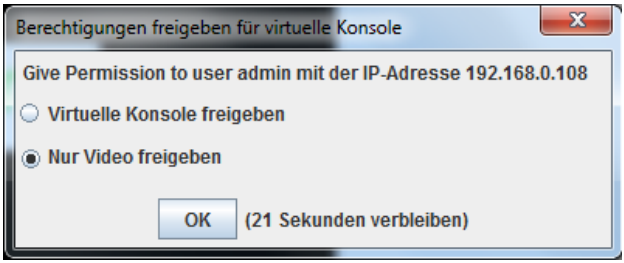

Berechtigungen freigeben für virtuelle Konsole
Give Permission to user admin mit der IP-Adresse 192.168.0.108
Virtuelle Konsole freigeben
Nur Video freigeben
OK
(21 Sekunden verbleiben)

Bild 26: Dialogfenster Berechtigungen freigeben für virtuelle Konsole - Give Permission to user admin ...

Dieses Dialogfenster, das von 28 Sekunden herunter rechnet, bietet die folgende Optionen zur Auswahl, die durch Klicken auf *OK* aktiviert werden können:

*Virtuelle Konsole freigeben*

Der AVR-Sitzung 1 wurde *Vollzugriff* erteilt. In der AVR-Sitzung 1 wird dies wie folgt angezeigt:

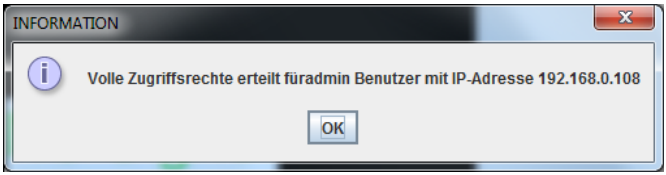



Bild 27: Dialogfenster INFORMATION - "Vollzugriff" erteilt

*Nur Video freigeben*

Die AVR-Sitzung 1 verbleibt im *Teilzugriff (nur Video)*-Modus (Standard). In der AVR-Sitzung 1 wird dies wie folgt angezeigt:

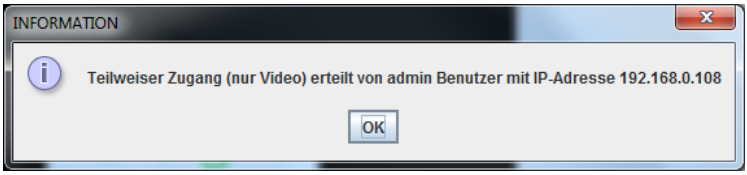



Bild 28: Dialogfenster INFORMATION "Teilzugriff (nur Video)" erteilt

### "Vollzugriff"-Sitzung beenden

Wenn derzeit zwei AVR-Sitzungen aktiv sind und Sie die Sitzung im *Vollzugriff*-Modus schließen, wird das folgende Dialogfenster geöffnet, in dem Sie aufgefordert werden, die nächste Mastersitzung auszuwählen (d. h. die Sitzung mit *Vollzugriff*).

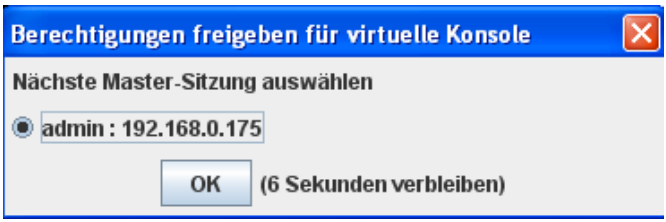



Bild 29: Dialogfenster Berechtigungen freigeben für virtuelle Konsole - Nächste Master-Sitzung auswählen

In diesem Dialogfenster, in dem von 10 Sekunden heruntergezählt wird, wird der Benutzer der anderen Sitzung zur Auswahl angezeigt.

– Wenn Sie diese Option wählen, wechselt die andere Sitzung in den *Vollzugriff*-Modus.

– Wenn Sie diese Option deaktivieren, bleibt die andere Sitzung im *Teilzugriff (nur Video)*-Modus.

– Wenn der Zähler abläuft, bevor Sie mit *OK* bestätigt haben, bleibt die andere Sitzung im *Teilzugriff (nur Video)*-Modus.

## 5.2.4 „Lokaler Bildschim Aus Kontrolle“-Funktionalität

Die Funktionalität *Lokaler Bildschim Aus Kontrolle* des iRMC S4 bietet Ihnen die Möglichkeit, den lokalen Monitor des verwalteten Servers für die Dauer Ihrer AVR-Sitzung auszuschalten. Auf diese Weise stellen Sie sicher, dass am lokalen Bildschirm des Servers Ihre via AVR durchgeführten Eingaben und Aktionen nicht sichtbar sind. Am Server wird „Lokaler Bildschirm aus“ durch Blinken der Identifizierungs-LED signalisiert.

Die Funktionalität *Lokaler Bildschim Aus Kontrolle* konfigurieren Sie über die Seite *Grafische Konsolen Umleitung (AVR)* der iRMC S4-Weboberfläche (siehe Seite 346). Auf der Seite *Grafische Konsolen Umleitung (AVR)* können Sie zusätzlich konfigurieren, dass sich der lokale Bildschirm beim Start einer neuen AVR-Sitzung immer automatisch ausschaltet.

Nachdem Sie das System entsprechend konfiguriert haben, können Sie den lokalen Monitor des Servers über die Remote-Workstation ein- und ausschalten, indem Sie alternativ das AVR-Menü *Video* verwenden, indem Sie in der Symbolleiste auf das zweite Symbol von rechts klicken.

Der lokale Monitor ist immer eingeschaltet und kann nicht ausgeschaltet werden, wenn die Option *Lokaler Bildschirm Aus Kontrolle* (siehe Seite 351) deaktiviert ist.

Der aktuelle Status des lokalen Monitors wird im AVR-Menü *Video* und über das zweite Symbol von rechts in der AVR-Symbolleiste angezeigt (siehe Abschnitt "AVR-Symbolleiste" auf Seite 118):

| | |
|---|---|
| | Gibt an, dass der lokale Monitor gesperrt (abgeschaltet) ist, d. h. über die AVR-Konsole durchgeführte Aktionen werden nicht auf dem Monitor des verwalteten Servers angezeigt. Wenn Sie auf diese Schaltfläche klicken, wird der Monitor des verwalteten Servers entsperrt, und die Symbolfarbe ändert sich in Grün. |
| | Gibt an, dass der lokale Monitor entsperrt (eingeschaltet) ist, d. h. über die AVR-Konsole durchgeführte Aktionen werden auf dem Monitor des verwalteten Servers angezeigt. Wenn Sie auf diese Schaltfläche klicken, wird der Monitor des verwalteten Servers gesperrt, und die Symbolfarbe ändert sich in Rot.<br><br>Wenn die Option *Lokalen Monitor kontrollieren* deaktiviert ist (siehe Seite 351), kann der Monitorstatus nicht umgeschaltet werden. |

## 5.2.5 Umleitung der Tastatur

Die Tastatur-Umleitung funktioniert nur, wenn das AVR-Fenster den Eingabe-Fokus hat:

- Falls die Tastatur-Umleitung nicht zu funktionieren scheint, klicken Sie einfach auf das AVR-Fenster.
- Falls die Tastatur nicht reagiert, überprüfen Sie, ob sich das AVR-Fenster im „Nur Lesen“-Modus befindet. Wie Sie in den „Volle Kontrolle“-Modus umschalten, ist auf Seite 89 beschrieben.

### Besondere Tastenkombinationen

AVR überträgt alle normalen Tastenkombinationen an den Server. Sondertasten, wie z. B. Windows-Tasten, werden nicht übertragen. Einige spezielle Tastenkombinationen, wie z. B. ALT + F4, können nicht übertragen werden, da sie vom Betriebssystem des Client abgefangen werden. In diesen Fällen behelfen Sie sich mit den integrierten Sondertasten, den selbst definierten Hotkeys oder der virtuellen Tastatur.

### Vollständige Tastatur-Unterstützung

Mit der Funktion *Full keyboard support* können Sie alle Funktionstasten der physikalischen Tastatur des verwalteten Servers via *SoftKeyboard* verwenden.

### Integrierte Sondertasten

Rechts unten  im AVR-Fenster finden Sie die Leiste mit den Sondertasten. Diese Tasten sind als „Sticky Keys“ implementiert, d.h. sie bleiben nach Anklicken „gedrückt“ (rot gekennzeichnet) und werden erst durch erneutes Anklicken in die Grundstellung zurückgesetzt.

Mithilfe der integrierten Sondertasten können Sie z.B. spezielle Tastenkombinationen nutzen, die bei Eingabe über Ihre Tastatur nicht via AVR übertragen werden können.

Bild 30: AVR-Fenster - Integrierte Sondertasten

LALT
: Linke Alt(ernate)-Taste (entspricht der Taste Alt auf Ihrer Tastatur).

[LCTRL]
Linke Steuerungstaste (entspricht der linken Taste [Strg] (Ctrl) auf Ihrer Tastatur).

[RALT]
Rechte Alt(ernate)-Taste / Alt(ernate) Graphic-Taste (entspricht der Taste [Alt Gr] auf Ihrer Tastatur).

[RCTRL]
Rechte Steuerungstaste (entspricht der rechten Taste [Strg] (Ctrl) auf Ihrer Tastatur).

[Num]
Num-Taste. Aktiviert/deaktiviert die numerischen Tasten rechts auf Ihrer Tastatur (entspricht der Taste [Num] auf Ihrer Tastatur).

[Caps]
Feststelltaste (entspricht der Taste [Caps Lock] auf Ihrer Tastatur).

[Scroll]
Scroll-Taste Entspricht der Taste [Rollen] auf Ihrer Tastatur.

### SoftKeyboard (virtuelle Tastatur)

Das SoftKeyboard (auch bekannt als virtuelle Tastatur, siehe Bild 31) bietet Ihnen eine bedienbare Darstellung einer Tastatur. Bei Verwendung des SoftKeyboards stehen Ihnen alle Tastenkombination zur Verfügung. Somit können Sie das SoftKeyboard als vollwertige Alternative für eine reale Tastatur verwenden.

Das SoftKeyboard aktivieren Sie im AVR-Fenster über das Menü *Tastatur* (siehe Seite 98).

virtuelle Tastatur - Deutsch(Deutschland)
esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 psc slk brk
^ 1 2 3 4 5 6 7 8 9 0 ß ´ bksp ins hm pup nlk / * -
tab q w e r t z u i o p ü + # del end pdn 7 8 9 +
caps a s d f g h j k l ö ä ent 4 5 6
shift < y x c v b n m , . - shift ^ 1 2 3 ent
ctrl win alt CM alt win ctrl <= v => 0 .
Bild 31: SoftKeyboard (Tastaturlayout: Englisch (US))

### Sichere Tastatur (Secure Keyboard)

Wenn Sie über eine HTTP-Verbindung mit der iRMC S4-Weboberfläche verbunden sind, können Ihre Tastatureingaben und Mausklicks so konfiguriert werden, dass sie in Echzeit verschlüsselt werden, bevor sie an den verwalteten Server übermittelt werden (siehe Abschnitt "AVR-Fenster - Menü „Optionen“" auf Seite 111).

### 5.2.6 Umleitung der Maus

Der Mauszeiger des verwalteten Servers wird synchron mit der Maus am Remote-Arbeitsplatz bewegt. Die Mausumleitungseinstellungen konfigurieren Sie im AVR-Fenster unter *Maus-Modus* im Menü *Maus* (siehe Seite 109).

Die Einstellungen für die Mauszeiger-Synchronisation werden nur für das Betriebssystem unterstützt, das auf dem verwalteten Server läuft.

Falls die Software zur Steuerung des Mauszeigers aktiv ist, kann der Mauszeiger nicht immer synchronisiert werden.

### 5.2.7 Menüs und Symbolleiste des AVR-Fensters

Die Menüleiste des AVR-Fensters enthält folgende Menüs:

- Über das Menü *Video* können Sie die Einstellungen der AVR konfigurieren und die AVR steuern (siehe Seite 98).
- Über das Menü *Tastatur* können Sie das *SoftKeyboard* aktivieren und die Tastatursprache auswählen. Darüber hinaus können Sie über das Menü *Tastatur* Sondertasten für die Umleitung der Tastaturen auswählen (siehe Seite 102).
- Über das Menü *Maus* können Sie die Mauseinstellungen konfigurieren (siehe Seite 109).
- Über das Menü *Optionen* können Sie die Tastaturverschlüsselung aktivieren und deaktivieren, die Fenstergröße an Ihre Bedürfnisse anpassen und die Sprache (Deutsch, Englisch, Japanisch) auswählen, in der die Menüs und Dialogfenster des AVR-Fensters angezeigt werden sollen (siehe Seite 111). Zusätzlich können Sie über das Menü *Optionen* die volle Berechtigung anfordern (*Vollzugriff*-Modus), wenn Ihre AVR-Sitzung diejenige von zwei gleichzeitig laufenden AVR-Sitzungen ist, die in *Teilzugriff (nur Video)*-Modus läuft.
- Über das Menü *Medien* können Sie den *Virtuelle Medien Wizard* aufrufen (siehe Seite 113).
- Das Menü *Ein-/Ausschalten* ermöglicht es Ihnen, den verwalteten Server ein- und auszuschalten und das Verhalten des Servers beim nächsten Boot-Vorgang festzulegen (siehe Seite 114).
- Das Menü *Aktive Benutzer* enthält die derzeit aktiven AVR-Sitzungen (siehe Seite 116).

– Über das Menü *Hilfe* können Sie Informationen zu der Version des derzeit ausgeführten KVM Remote Console-Hilfsprogramms sowie Informationen zum verwalteten Server anzeigen (siehe Seite 116).

Die Symbole der AVR-Symbolleiste bieten einen direkten Zugriff auf häufig verwendete AVR-Funktionen.

### 5.2.7.1 Menü Video

Über das Menü *Video* können Sie die AVR-Einstellungen konfigurieren und die AVR steuern.

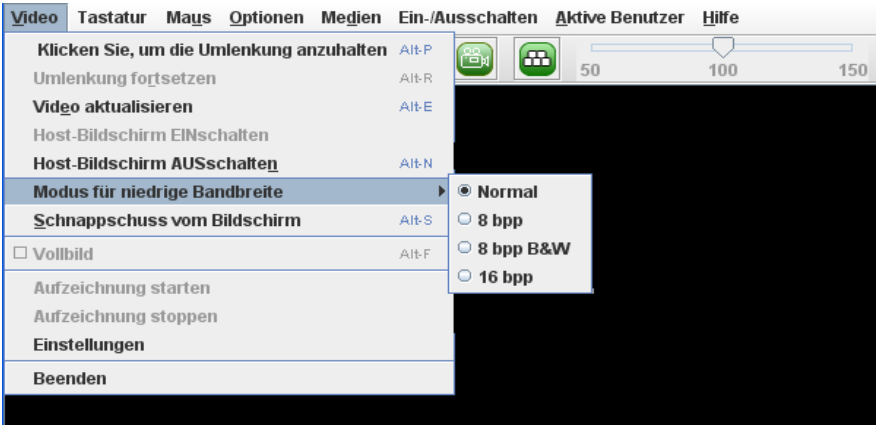



Bild 32: AVR-Fenster - Menü „Video“

Im Menü *Video* können Sie die folgenden Funktionen auswählen:

*Klicken Sie, um die Umlenkung anzuhalten*
: Hält die AVR an und fixiert die AVR-Ansicht. Die AVR-Ansicht bleibt solange fixiert, bis die AVR fortgesetzt wird.

*Umlenkung fortsetzen*
: Setzt die AVR fort und aktualisiert die AVR-Ansicht.

*Video aktualisieren*
: Aktualisiert die AVR-Ansicht.

*Host-Bildschirm EINschalten*
: Schaltet, je nachdem ob diese Option ausgewählt wurde, den lokalen Monitor des verwalteten Servers ein.

Auch wenn der lokale Bildschirm ausgeschaltet ist, ist die Funktion in folgenden Fällen deaktiviert:

- Sie befinden sich im „Nur Lesen“-Modus.
- Am verwalteten Server ist ein Grafikmodus mit hohe Auflösung eingestellt (siehe Tabelle 3 auf Seite 84).
  Lokaler Bildschirm <status>-Anzeige: *Lokaler Bildschirm ist immer aus*

*Host-Bildschirm AUSschalten*

Schaltet, je nachdem ob diese Option ausgewählt wurde, den lokalen Monitor des verwalteten Servers aus.

Wenn Sie sich im „Nur Lesen“-Modus befinden, ist diese Funktion deaktiviert, selbst wenn der lokale Monitor ausgeschaltet ist.

*Modus für niedrige Bandbreite*

Im Falle einer reduzierten Übertragungsrate können Sie hier für alle AVR-Sitzungen am selben iRMC S4 eine verringerte Bandbreite (Einheit: bits per pixel, bpp) hinsichtlich der Farbtiefe einstellen.

*Normal*

Voreinstellung.
Keine reduzierte Bandbreite.

*8 bpp*

8 bpp Farbtiefe (256 Farbstufen).

*8 bpp B&W*

8 bpp Schwarzweiß-Tiefe (256 Graustufen).

*16 bpp*

16 bpp Farbtiefe (65 536 Farbstufen).

*Schnappschuss vom Bildschirm*

Erstellt einen Screenshot der AVR-Ansicht und öffnet einen Dateibrowser, über den Sie die entsprechende Datei *CapturedScreen.jpeg* in einem Verzeichnis Ihrer Workstation oder auf einem Netzlaufwerk speichern können.

Dieselbe Funktionalität steht auch zur Verfügung über die Seite *Advanced Video Redirection* der iRMC S4 Weboberfläche (siehe "Bildschirm-Abbild erstellen" auf Seite 348).

*Vollbild*

Schaltet den Vollbildmodus ein oder aus.

Diese Option ist nur aktiviert, wenn die Bildschirmauflösung der Remote-Workstation mit der Bildschirmauflösung des verwalteten Servers übereinstimmt.

*Aufzeichnung starten*

Erstellt eine Video-Aufzeichnung der Ereignisse, die am Monitor des verwalteten Servers angezeigt werden.

Diese Schaltfläche ist in folgenden Fällen deaktiviert:

- Sie haben noch nicht die Video-Einstellungen unter der Option *Einstellungen* (siehe unten) konfiguriert.
- Derzeit wird eine Video-Aufzeichnung ausgeführt.

*Aufzeichnung stoppen*

Stoppt eine Video-Aufzeichnung. Diese Option ist nur aktiviert, wenn derzeit eine Video-Aufzeichnungssitzung läuft.

*Einstellungen*

Öffnet das Dialogfenster *Video-Aufzeichnung*, in dem Sie die Einstellungen für die Aufzeichnung eines Videos konfigurieren können.

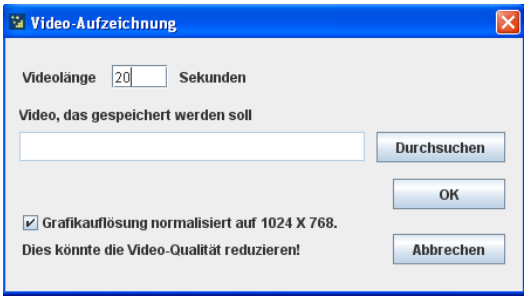



Bild 33: Einstellung für Video-Aufzeichnung

*Videolänge*

Dauer des Videos (in Sekunden)

*Durchsuchen...*

Öffnet ein Browserfenster, in dem Sie zu einem Verzeichnis auf Ihrem Computer oder einem Netzlaufwerk navigieren können, in dem das Video gespeichert werden soll.

*Video, das gespeichert werden soll*

Zeigt das von Ihnen über *Durchsuchen* ausgewählte Verzeichnis.

*Grafikauflösung normalisiert auf 1024x768*

In diesem Fall wird eine eigene Videodatei für jede Auflösungsänderung am Monitor des verwalteten Servers erstellt.

Wenn diese Option aktiviert ist, wird eine normalisierte Videoauflösung von 1024x768 auf die gesamte Grafikauflösung angewendet, unabhängig von der tatsächlichen Grafikauflösung des Monitors des verwalteten Servers. Dies könnte die Video-Qualität reduzieren.

*OK*

Aktiviert Ihre Einstellungen und schließt den Dialog. Die Schaltfläche *Aufzeichnung starten* ist nun aktiviert.

*Abbrechen*

Schließt das Dialogfenster, ohne dass Ihre Einstellungen aktiviert wurden.

*Beenden*

Beendet die eigene AVR-Sitzung.

### 5.2.7.2 AVR-Fenster - Menü „Tastatur“

Über das Menü *Tastatur* können Sie Sondertasten für die Umleitung der Tastaturen auswählen (siehe Abschnitt "Umleitung der Tastatur" auf Seite 93).

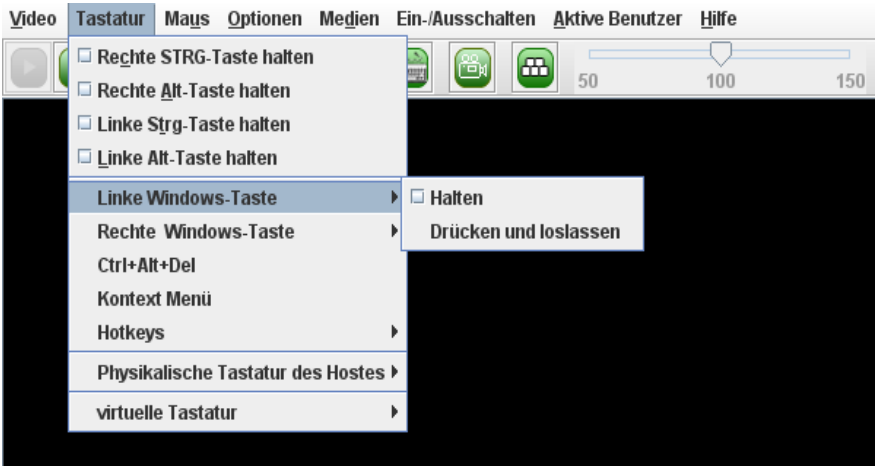



Bild 34: AVR-Fenster - Menü „Tastatur“

Im Menü *Tastatur* können Sie die folgenden Funktionen auswählen:

*Rechte Strg-Taste halten*
: Hält die rechte Strg-Taste gedrückt.

*Rechte Alt-Taste halten*
: Hält die rechte Alt-Taste gedrückt.

*Linke Strg-Taste halten*
: Hält die linke Strg-Taste gedrückt.

*Linke Alt-Taste halten*
: Hält die linke Alt-Taste gedrückt.

*Linke Windows-Taste*
: Hält die linke Windows-Taste gedrückt, wenn *Halten* aktiviert ist. Anderenfalls gilt die Aktion *Drücken und loslassen*.

*Rechte Windows-Taste*
: Hält die rechte Windows-Taste gedrückt, wenn *Halten* aktiviert ist. Anderenfalls gilt die Aktion *Drücken und loslassen*.

*Ctrl+Alt+Del*

Wendet den Tastaturbefehl Strg + Alt + Entf an.

*Kontext Menü*

Öffnet das entsprechende Kontextmenü der Anwendung oder des Betriebssystems, das auf dem verwalteten Server ausgeführt wird.

*Hotkeys*

Ermöglicht es Ihnen, Ihre eigenen Hotkeys zu definieren und anzuwenden.

Gehen Sie folgendermaßen vor, um einen bereits definierten Hotkey anzuwenden.

1. Klicken Sie auf *Hotkeys*.

   Zum Definieren der Hotkeys können Sie auch das Symbol *Hotkey* in der AVR-Symbolleiste verwenden (siehe Abschnitt "AVR-Symbolleiste" auf Seite 118).

2. Klicken Sie in der Liste der bereits definierten Hotkeys, die unter dem Element *Add Hot Key* angezeigt wird, auf den gewünschten Hotkey.

Gehen Sie folgendermaßen vor, um einen neuen Hotkey zu definieren:

1. Klicken Sie auf *Hotkeys – Add Hot Key*.

   Das Dialogfenster *Benutzerdefinierte Makros* wird geöffnet, in dem die bereits definierten benutzerdefinierten Makros angezeigt werden (Beispiel: A, B):

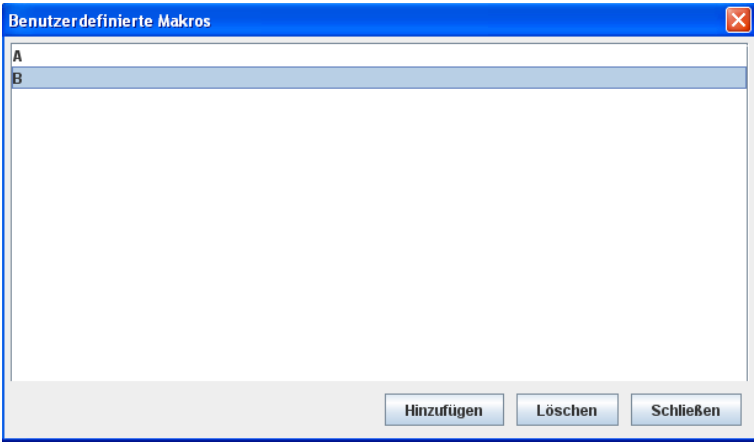



Bild 35: AVR-Fenster - Menü „Tastatur“ - Add Hot Key - Benutzerdefinierte Makros (1)

2. Klicken Sie auf *Hinzufügen*, um ein neues benutzerdefiniertes Makro zu definieren.

   Das Dialogfenster *Makro hinzufügen* wird geöffnet:

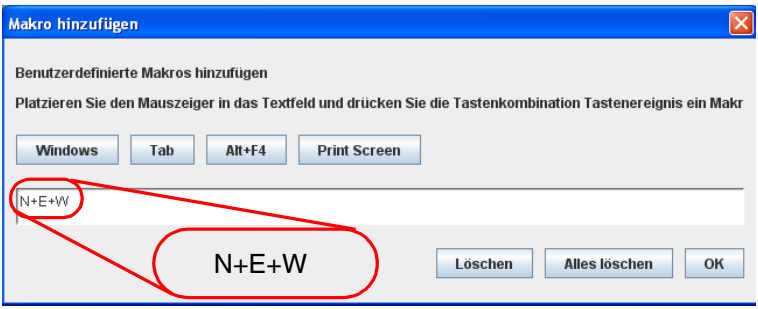



Bild 36: AVR-Fenster - Menü „Tastatur“ - Add Hot Key - Makro hinzufügen

3. Geben Sie Ihre bevorzugte Kombination bestehend aus bis zu sechs Tasten ein, indem Sie die *Windows*-, *Tab*-, *Alt+F4*- und *Print Screen*-Schaltflächen verwenden und/oder die Tasten Ihrer Tastatur drücken.

   Die eingegebene Tastenkombination wird im Dialogfenster *Makro hinzufügen* angezeigt. Wenn Sie auf *Alles löschen* oder *Löschen* klicken, können Sie die gesamte Eingabe bzw. die ganz rechts stehende Tasteneingabe entfernen, wenn Sie jeweils auf *Alles löschen* oder *Löschen* klicken.

4. Klicken Sie auf *OK*, um den neuen Hotkey zu aktivieren.

   Der neue Hotkey wird jetzt im Dialogfenster *Benutzerdefinierte Makros* angezeigt:

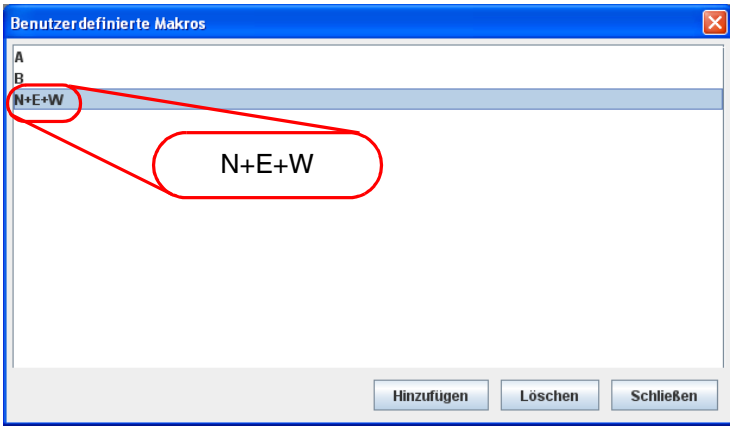



Bild 37: AVR-Fenster - Menü „Tastatur“ - Add Hot Key - Benutzerdefinierte Makros (2)

5. Wählen Sie zum Entfernen eines Hotkeys den entsprechenden Eintrag aus (z. B. „B“ wie im Beispiel in Bild 37 auf Seite 106) und klicken Sie auf *Löschen*.

6. Klicken Sie auf *Schließen*, um das Dialogfenster *Benutzerdefinierte Makros* zu schließen.

*Physikalische Tastatur des Hostes*

Sprache, die für die Tastatur des verwalteten Servers verwendet wird.

Die folgenden Optionen stehen zur Verfügung:

- *Auto Detect* (Standardwert)
- *Englisch (US)*
- *Englisch (UK)*
- *Französisch*
- *Französisch (Belgien)*
- *Deutsch (Deutschland)*
- *Deutsch (Schweiz)*
- *Japanisch*
- *Spanisch*
- *Italienisch*
- *Dänisch*
- *Finnisch*
- *Norwegisch (Norwegen)*
- *Portugiesisch (Portugal)*
- *Schwedish*
- *Niederländisch (Niederlande)*
- *Niederländisch (Belgien)*
- *Türkisch - F*
- *Türkisch - Q*

Wenn Sie *Auto Detect* auswählen, geht AVR davon aus, dass die Tastatursprache der Sprache des verwalteten Servers und der Remote-Workstation entspricht.

*SoftKeyboard*

Zeigt das SoftKeyboard (d. h. die virtuelle Tastatur) an.

Gehen Sie folgendermaßen vor, um das SoftKeyboard in der bevorzugten Sprache anzuzeigen:

1. Zeigen Sie mit dem Mauszeiger auf das Element *SoftKeyboard*.

   Es wird eine Liste der verfügbaren SoftKeyboard-Sprachen angezeigt.

2. Wählen Sie die bevorzugte Sprache aus der Liste aus.

   Das SoftKeyboard wird für die ausgewählte Sprache angezeigt:

virtuelle Tastatur - Deutsch(Deutschland)
esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 psc slk brk
^ 1 2 3 4 5 6 7 8 9 0 ß ´ bksp ins hm pup nlk / * -
tab q w e r t z u i o p ü + # del end pdn 7 8 9 +
caps a s d f g h j k l ö ä ent 4 5 6
shift < y x c v b n m , . - shift ^ 1 2 3 ent
ctrl win alt CM alt win ctrl <= v => 0 .

Bild 38: AVR-Fenster - Menü „Tastatur“ - SoftKeyboard

*Full Keyboard Support*

Wenn aktiviert, können Sie über *SoftKeyboard* alle Funktionstasten der physikalischen Tastatur des verwalteten Servers verwenden.

### 5.2.7.3 AVR-Fenster - Menü „Maus“

Über das Menü *Maus* können Sie die Einstellungen für die Umleitung der Maus konfigurieren.

Bild 39: AVR-Fenster - Menü „Maus“

Im Menü *Maus* können Sie die folgenden Funktionen auswählen:

*Mauszeiger anzeigen*
: Blendet den Mauszeiger der Remote-Workstation bei der Arbeit mit AVR ein bzw. aus.

*Maus-Kalibrierung*
: Wird für das Kalibrieren des relativen Maus-Modus verwendet. Diese Option ist nur aktiviert, wenn *Maus-Modus* - *Relativer Maus-Modus* ausgewählt wurde.

> **i** Im relativen Maus-Modus folgt der Mauszeiger des verwalteten Servers dem Mauszeiger der Remote-Workstation langsamer.

*Host-Mauszeiger anzeigen*
: Blendet einen zusätzlichen Mauszeiger neben dem Mauszeiger des verwalteten Servers ein.

> **i** Wenn die Hardwarebeschleunigung des Mauszeigers auf den Maximalwert eingestellt ist und der Matrox G200e-Treiber installiert ist, wird der Hardware-Mauszeiger des iRMC S4 aktiviert. Es wird normalerweise nur ein Mauszeiger in diesem Modus angezeigt. In diesem Fall kann die Option *Host-Mauszeiger anzeigen* dazu verwendet werden, einen zweiten Mauszeiger für den verwalteten Server anzuzeigen.

*Maus-Modus*

Über diese Option können Sie den Maus-Modus auswählen (*Absoluter Maus-Modus*, *Relativer Maus-Modus* oder *Lokale Maus verbergen*). Im Modus *Lokale Maus verbergen* wird der Mauszeiger der Remote-Workstation nicht angezeigt.

Standardeinstellung: *Absoluter Maus-Modus.*

Verwenden Sie immer die Option *Absoluter Maus-Modus*. Nur bei einem älteren Betriebssystem (z. B. RedHat 4) kann es sein, dass die Option *Absoluter Maus-Modus* nicht funktioniert.

Bei LSI WEBBIOS muss die Option *Lokale Maus verbergen (Relativ)* verwendet werden.

### 5.2.7.4 AVR-Fenster - Menü „Optionen“

Über das Menü *Optionen* können Sie die Tastatur-/Mausverschlüsselung aktivieren und deaktivieren, die Fenstergröße an Ihre Bedürfnisse anpassen und die Sprache auswählen, in der die Menüs und Dialogfenster des AVR-Fensters angezeigt werden sollen.

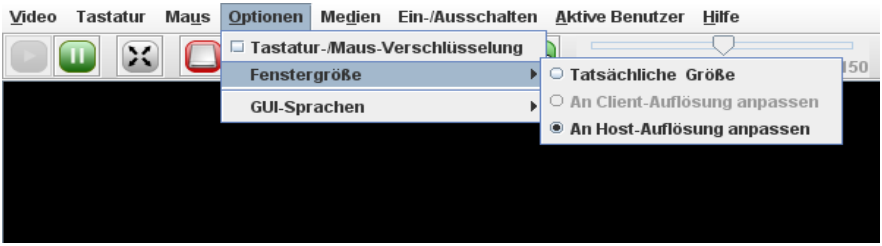



Bild 40: AVR-Fenster - Menü „Optionen“

Im Menü *Optionen* können Sie die folgenden Funktionen auswählen:

*Tastatur-/Maus-Verschlüsselung*

Aktiviert bzw. deaktiviert die Tastatur-/Mausverschlüsselung, die dafür sorgt, dass Ihre Tastatureingaben und Mausklicks in Echtzeit verschlüsselt werden, bevor sie an den verwalteten Server übermittelt werden.

Diese Option steht nicht zur Auswahl, wenn Sie über eine HTTPS-Verbindung mit der iRMC S4-Weboberfläche verbunden sind. In diesem Fall wird die gesamte Kommunikation zwischen der iRMC S4-Weboberfläche und dem verwalteten Server mittels SSL verschlüsselt.

*Fenstergröße*

Bestimmt, ob das AVR-Fenster in der tatsächlichen Größe angezeigt werden soll oder ob die Größe an die Auflösung des lokalen Monitors des verwalteten Servers oder an die Monitorauflösung der Remote-Workstation angepasst werden soll.

*Tatsächliche Größe*

Das AVR-Fenster hat dieselbe Größe wie der Monitor.

*An Host-Auflösung anpassen*

Diese Option ist nur aktiviert, wenn die Bildschirmauflösung der Remote-Workstation geringer oder gleich der Bildschirmauflösung des verwalteten Servers ist.

Wenn die Bildschirmauflösung der Remote-Workstation und des verwalteten Servers identisch sind, wird das Symbol *Vollbild* in der AVR-Symbolleiste aktiviert (siehe Abschnitt "AVR-Symbolleiste" auf Seite 118).

*An Host-Auflösung anpassen*

Wenn die Bildschirmauflösung der Remote-Workstation höher ist als die Bildschirmauflösung des verwalteten Servers, wird das AVR-Fenster

automatisch angepasst.

Dies ist die normale Arbeitsumgebung.

*GUI-Sprachen*

Legt die Sprache fest, in der die Menüs und Dialogfenster des AVR-Fensters angezeigt werden sollen (*Deutsch*, *Englisch*, *Japanisch*).

Standardmäßig wird die GUI-Sprache ausgewählt, die für die iRMC S4-Weboberfläche konfiguriert wurde, von der aus die AVR-Sitzung gestartet wurde.

Fordert den Benutzer der gleichzeitig laufenden AVR-Sitzung auf, Ihnen *Vollzugriff* zu erteilen. Abhängig von der Entscheidung des Benutzers wird Ihnen *Vollzugriff* erteilt oder Sie bleiben im *Teilzugriff (nur Video)*-Modus.

*Volle Berechtigung anfordern*

Diese Option steht nur zur Auswahl, wenn zwei AVR-Sitzungen gleichzeitig aktiv sind und Ihre Sitzung diejenige ist, die sich nicht im *Vollzugriff*-Modus befindet.

Fordert den Benutzer der gleichzeitig laufenden AVR-Sitzung auf, Ihnen *Vollzugriff* zu erteilen. Abhängig von der Entscheidung des Benutzers wird Ihnen *Vollzugriff* erteilt oder Sie bleiben im *Teilzugriff (nur Video)*-Modus. Näheres hierzu finden Sie im ""Vollzugriff" anfordern wenn zwei AVR-Sitzungen gerade aktiv sind" auf Seite 89.

### 5.2.7.5 AVR-Fenster - Menü „Medien“

Über das Menü *Medien* können Sie den *Virtuelle Medien Wizard* starten. Mit dem *Virtuelle Medien Wizard* können Sie Medien auf der Remote-Workstation als virtuelle Mediengeräte anhängen oder von dort lösen (siehe Kapitel "Virtuelle Medien Wizard" auf Seite 123).

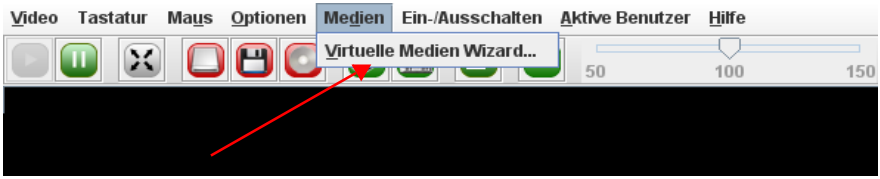



Bild 41: AVR-Fenster - Menü „Medien“

*Virtuelle Medien Wizard...*

Klicken Sie auf *Virtuelle Medien Wizard...*, um den *Virtuelle Medien*-Wizard zu starten, mit dem Sie Medien auf der Remote-Workstation als virtuelle Mediengeräte anhängen oder von dort lösen können (siehe Kapitel "Virtuelle Medien Wizard" auf Seite 123).

### 5.2.7.6 AVR -Fenster - Menü „Ein-/Ausschalten“

Über das Menü *Ein-/Ausschalten* können Sie den Server einschalten, ausschalten oder neu starten. Darüber hinaus können Sie das Verhalten des Servers beim nächsten Boot-Vorgang konfigurieren.

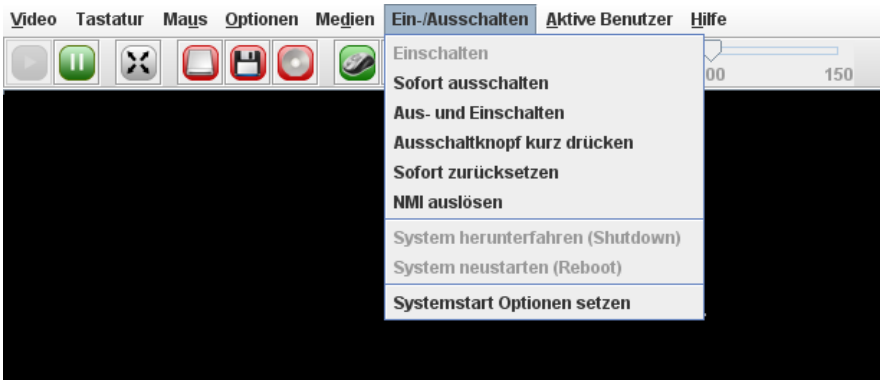



Bild 42: AVR -Fenster - Menü „Ein-/Ausschalten“

*Power On*

Schaltet den Server ein.

*Immediate Power Off*

Schaltet den Server aus unabhängig vom Status des Betriebssystems aus.

*Power Cycle*

Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein. Diese Zeit können Sie im Eingabefeld *Aus-/Einschalt Verzögerung* der Gruppe *ASR&R Einstellungen* (siehe Seite 264) konfigurieren.

*Ausschaltknopf kurz drücken*

Abhängig vom installierten Betriebssystem und der konfigurierten Aktion können Sie mit Ausschaltknopf kurz drücken unterschiedliche Aktionen auslösen wie Herunterfahren, Standby-Modus oder Ruhezustand auslösen. Mit diesen Aktionen können Sie den Computer ausschalten oder in den Standby-Modus schalten.

*Sofort zurücksetzen*

Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).

*NMI auslösen*

Löst eine nicht-maskierbare Unterbrechung (non-maskable interrupt, NMI) aus Ein NMI ist eine Prozessorunterbrechung, die nicht von Standard-Unterbrechungsmaskierung des Systems ignoriert werden kann.

*Graceful Reset (Reboot)*

Graceful Shutdown und Reboot.
Diese Option ist nur verfügbar, wenn die ServerView Agents installiert und beim iRMC S4 als „Connected“ gemeldet sind.

*Graceful Power Off (Shutdown)*

System „sanft“ herunterfahren und ausschalten.
Diese Option ist nur verfügbar, wenn die ServerView Agents installiert und beim iRMC S4 als „Connected“ gemeldet sind.

*Systemstart Optionen setzen*

Wenn Sie diese Option wählen, wird das Dialogfenster *Systemstart Optionen setzen* geöffnet, in dem Sie das Verhalten des Systems beim **nächsten** Neustart konfigurieren können.

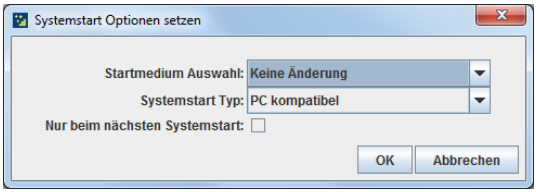



Bild 43: Menü „Ein-/Ausschalten“ - Systemstart Optionen setzen

*Startmedium Auswahl*

Speichermedium, von dem aus der Boot-Vorgang durchgeführt werden soll. Die folgenden Optionen stehen zur Verfügung:

- *Keine Änderung*: Das System wird von demselben Speichermedium aus wie zuvor gebootet.
- *PXE/iSCSI*: Das System wird über das Netzwerk von PXE/iSCSI gebootet.
- *Festplatte*: Das System wird von der Festplatte aus gebootet.
- *CDROM/DVD*: Das System wird von einer CD/DVD aus gebootet.
- *Diskette*: Das System wird von einer Diskette aus gebootet.

– *Bios Setup*: Beim Booten wird das System in das BIOS-Setup geschaltet.

*Boot Type*

Ermittelt den Boot-Modus in dem das System beim nächsten Booten gestartet wird.

Abhängig vom Betriebssystem des Servers, können folgende Optionen ausgewählt werden:

*PC compatible (legacy)*

Das System wird in BIOS-Kompatibilitätsmodus (legacy) gebootet.

*Extensible Firmware Interface Boot (EFI)*

Das System wird in UEFI-Boot-Modus gebootet (nur auf 64-Bit-Betriebssysteme).

*Nur beim nächsten Systemstart*

Die konfigurierten Einstellungen gelten nur für den nächsten Systemstart.

### 5.2.7.7 AVR -Fenster - Menü „Aktive Benutzer“

Das Menü *Aktive Benutzer* zeigt die Benutzer an, die derzeit AVR verwenden. Der grüne Punkt kennzeichnet Ihre eigene Sitzung.

Bild 44: AVR -Fenster - Menü „Aktive Benutzer“

### 5.2.7.8 AVR-Fenster - Menü „Hilfe“

Neben allgemeinen Informationen über JViewer bietet das Menü *Hilfe* über das Dialogfenster *Serverinformationen* die unter *Systeminformationen* auf der Seite *System Überblick* der iRMC S4-Weboberfläche definierten Informationen (siehe Abschnitt "System Überblick - Allgemeine Informationen zum Server" auf Seite 148).

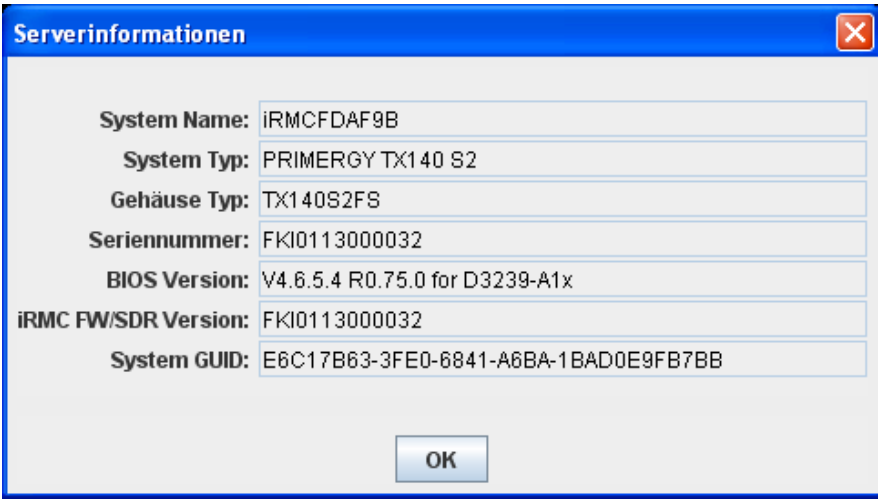



Bild 45: AVR-Fenster - Menü „Hilfe“

### 5.2.7.9 AVR-Symbolleiste

Die Symbole der AVR-Symbolleiste bieten einen direkten Zugriff auf häufig verwendete AVR-Funktionen. Wenn Sie mit dem Mauszeiger auf ein Symbol zeigen, werden oftmals QuickInfos mit weiteren Informationen angezeigt.

Im Modus *Teilzugriff (nur Video)* können nur die Symbole *Video* und *Aktive Benutzer* verwendet werden.

Bild 46: AVR-Fenster - Menü Präferenzen

Falls die Video-Umleitung Server-seitig im Modus *Num Lock On* ausgeführt wird, wechselt sie Client-seitig in den *Num Lock ON*.

Die folgende Liste zeigt die Symbole des Fensters *Server List* sowie deren Bedeutung:

| | |
|---|---|
| | Setzt die AVR fort und aktualisiert die AVR-Ansicht. |
| | Hält die AVR an und fixiert die AVR-Ansicht. Die AVR-Ansicht bleibt solange fixiert, bis die AVR fortgesetzt wird. |
| | Schaltet den Vollbildmodus ein oder aus. |
| | Gibt an, ob eine Festplatten-/USB-Umleitung für diese AVR-Sitzung eingerichtet wurde (grün) oder nicht (rot). Wenn Sie auf das Symbol klicken, wird der *Virtuelle Medien Wizard* gestartet (siehe Kapitel "Virtuelle Medien Wizard" auf Seite 123). |
| | Gibt an, ob eine Disketten-Umleitung für diese AVR-Sitzung eingerichtet wurde (grün) oder nicht (rot). Wenn Sie auf das Symbol klicken, wird der *Virtuelle Medien Wizard* gestartet (siehe Kapitel "Virtuelle Medien Wizard" auf Seite 123). |
| | Gibt an, ob eine CD-/DVD-Umleitung für diese AVR-Sitzung eingerichtet wurde (grün) oder nicht (rot). Wenn Sie auf das Symbol klicken, wird der *Virtuelle Medien Wizard* gestartet (siehe Kapitel "Virtuelle Medien Wizard" auf Seite 123). |

Tabelle 4: Symbole im Fenster „Server List“

| | |
|---|---|
| | Gibt an, ob der Mauszeiger der Remote-Workstation im AVR-Fenster sichtbar ist (grün) oder nicht (rot). Wenn Sie auf das Symbol klicken, können Sie zwischen den beiden Modi umschalten. |
| | Zeigt das SoftKeyboard an (Details siehe Abschnitt "AVR-Fenster - Menü „Tastatur“" auf Seite 102). |
| | Je nachdem, ob Video-Einstellungen konfiguriert wurden: Es wird eine Video-Aufzeichnung gestartet oder das Dialogfenster *Video-Aufzeichnung* wird geöffnet, um die Video-Einstellungen zu konfigurieren (Details siehe Abschnitt "Menü Video" auf Seite 98). |
| | Es wird eine Liste der verfügbaren Hotkeys angezeigt. Klicken Sie auf das entsprechende Element, um einen Hotkey anzuwenden. Informationen zum Definieren von Hotkeys finden Sie unter Abschnitt "AVR-Fenster - Menü „Tastatur“" auf Seite 102. |
| | Mit der Zoom-Symbolleiste können Sie die AVR-Ansicht stufenlos vergrößern oder verkleinern. |
| | Für jede derzeit aktive AVR-Sitzung werden der iRMC S4-Benutzer, der die AVR-Sitzung gestartet hat, sowie die IP-Adresse der Remote-Workstation, von der aus die AVR-Sitzung gestartet wurde, angezeigt. |
| <br> | Wenn *Lokaler Bildschim Aus Kontrolle* auf der AVR-Seite der iRMC S4-Weboberfläche aktiviert wurde, können Sie mit dieser Schaltfläche zwischen den folgenden Zuständen umschalten:<br><br>Gibt an, dass der Monitor des verwalteten Servers entsperrt ist, d. h. über die AVR-Konsole durchgeführte Aktionen werden am Monitor des verwalteten Servers angezeigt. Wenn Sie auf diese Schaltfläche klicken, wird der Monitor des verwalteten Servers gesperrt.<br><br>Gibt an, dass der Monitor des verwalteten Servers gesperrt ist, d. h. über die AVR-Konsole durchgeführte Aktionen werden nicht am Monitor des verwalteten Servers angezeigt. Wenn Sie auf diese Schaltfläche klicken, wird der Monitor des verwalteten Servers entsperren. |

Tabelle 4: Symbole im Fenster „Server List“

| | |
|---|---|
| | Mit dieser Schaltfläche können Sie den verwalteten Server ein- und ausschalten. |
| | Gibt an, dass der verwaltete Server derzeit eingeschaltet ist. Wenn Sie auf diese Schaltfläche klicken, wird ein Bestätigungsdialogfenster geöffnet, in dem Sie den verwaltete Server ausschalten (sofort ausschalten) können. |
| | Gibt an, dass der verwaltete Server derzeit ausgeschaltet ist. Wenn Sie auf diese Schaltfläche klicken, wird ein Bestätigungsdialogfenster geöffnet, in dem Sie den verwaltete Server einschalten können. |

Tabelle 4: Symbole im Fenster „Server List“

## 5.3 AVR über HTML5 verwenden

Zum Starten der AVR haben Sie folgende Möglichkeiten:

- Klicken Sie auf die Schaltfläche Video Umleitung starten (HTML5) auf der Seite Grafische Konsolen Umleitung (AVR) der iRMC-Weboberfläche (siehe Seite 346)

  oder, wenn angezeigt,

- Klicken Sie auf den Link *Video Umleitung (HTML5)* in der Baumstruktur der iRMC-Weboberfläche.

  Der Standard-Browser öffnet sich mit der Anzeige auf dem verwalteten Server.

Bild 47: Standard-Browser für AVR-Umleitung mit HTML5

Die HTML5-Seite ist in verschiedene Bereiche unterteilt:

### KVM-Einstellungen

In diesem Bereich können Sie Umleitung via HTML5 einstellen.

*Server IP*
: IP-Adresse des Servers, auf dem sich der iRMC befindet.

*Tastatur Layout*
Definiert, wie die Tastenanschläge auf der physikalischen Tastatur interpretiert werden. Sie haben zwei Möglichkeiten:

– Englisch (US)

– Deutsch

*Stop KVM*
Stoppt die Video-Umleitung.

*Ctrl&Alt&Del*
Führt Ctrl+Alt+Del auf dem Server aus.

*Record Video*
Zeichnet die umgeleitete Sitzung auf.

### Media Redirection

In dieser Gruppe können Sie Medien auf der Remote-Workstation als virtuelle Mediengeräte anhängen oder von dort lösen.

*CD Image*
Zeigt das ausgewählte ISO-Image an.

*Durchsuchen...*
Öffnet ein Dialogfenster, in dem Sie zum Verzeichnis des Speichermediums navigieren können, das Sie als virtuelles Medium von Ihrer Remote-Workstation aus zur Verfügung stellen möchten.

*Start Media Redirection*
Startet die Medien-Umleitung und verbindet das zur Verfügung gestellte Speichermedium als virtuelles Medium (Virtual Media).

### Unterstützte Browser

Die Funktion HTML5-Video-Umleitung wird von folgenden Browsern unterstützt:

– Microsoft Internet Explorer ab Version 11

– Modzilla Firefox ab Version 32

# 6 Virtuelle Medien Wizard

Für die Nutzung des Virtuelle Medien Wizards ist ein gültiger VM-Lizenzschlüssel (virtuelle Medien) erforderlich.

Der Virtuelle Medien Wizard stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, dessen Quelle Sie auf einer Remote-Workstation bereitstellen. Die virtuelle Medien-Verbindung zwischen dem verwalteten Server und der Remote-Workstation wird mit dem AVR-Java-Applet hergestellt. Abhängig von den Einstellungen auf der Seite *Virtual Media Optionen* können Sie bis zu 12 virtuelle Medien verbinden und zwischen folgenden Typen wählen:

– Physikalische Disketten und/oder Disketten-Images (bis zu 4)

– Physikalische CD/DVDs und/oder CD/DVD-ISO-Images (bis zu insgesamt 4)

– Festplattenlaufwerke und/oder Festplatten-/USB-Images (bis zu insgesamt 4)

Es ist nicht erforderlich, dass die Remote-Medien sich physikalisch auf der Remote-Workstation befinden. Sie können sich auch auf einem beliebigen Netzlaufwerk befinden, das von dieser Remote-Workstation aus zugängig ist.

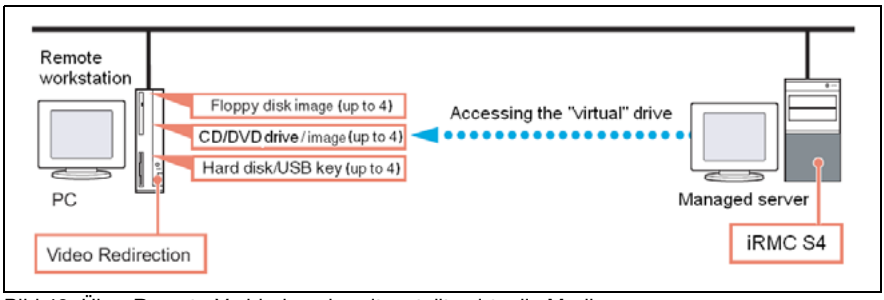



Bild 48: Über Remote-Verbindung bereitgestellte virtuelle Medien

# 6.1 Virtuelle Medien auf Remote-Workstation bereitstellen

Wenn Sie die Quelle für ein virtuelles Laufwerk auf der Remote-Workstation bereitstellen, unterstützt die virtuelle Funktion folgende Gerätetypen:

– Diskette
– CD-ISO-Image
– DVD-ISO-Image
– CD, DVD

Optische Speichermedien (CD, DVD) werden automatisch angezeigt (d.h. zur Auswahl angeboten).

Geräte, die als virtuelle Medien verbunden sind, werden vom iRMC S4 als USB-Geräte erkannt. Die Geräte können nicht verwendet werden, falls keine USB-Verbindung verfügbar ist (z.B weil kein USB-Treiber vorhanden ist).

Mithilfe des virtuellen Laufwerks können Sie vom Remote-Arbeitsplatz aus auf Ihrem PRIMERGY Server ein Betriebssystem installieren (siehe Kapitel "Remote-Installation des Betriebssystems via iRMC S4" auf Seite 439).

Der vorliegende Abschnitt informiert über folgende Themen:

- Virtuelle Medien Wizard starten
- Virtuelle Medien über Dialogfenster *Virtuelle Medien* handhaben
  - Speichermedien für die Virtuelle-Medien-Sitzung bereitstellen
  - Speichermedien als virtuelle Medien verbinden
  - Virtuelle Medien-Verbindungen löschen

### 6.1.1 Virtuelle Medien Wizard starten

Sie starten den Virtuelle Medien Wizard über das AVR-Java-Applet (siehe Abschnitt "Advanced Video Redirection - Advanced Video Redirection (AVR) starten" auf Seite 346).

- Starten Sie die iRMC S4-Weboberfläche (siehe Abschnitt "An der iRMC-Weboberfläche anmelden" auf Seite 134).
- Öffnen Sie die Seite *Grafische Konsolen Umleitung (AVR)* und klicken Sie auf die Schaltfläche *Video Umleitung starten (Java Web-Start)* , um die grafische Konsolen-Umleitung zu starten (siehe Abschnitt "Advanced Video Redirection - Advanced Video Redirection (AVR) starten" auf Seite 346).

  Das AVR-Fenster wird geöffnet.
- Wählen Sie in der Menüleiste des AVR-Fensters:
  *Medien - Virtuelle Medien Wizard...*

  oder klicken Sie auf eines der drei Symbole in der Symbolleiste *Virtuelle Medien*.

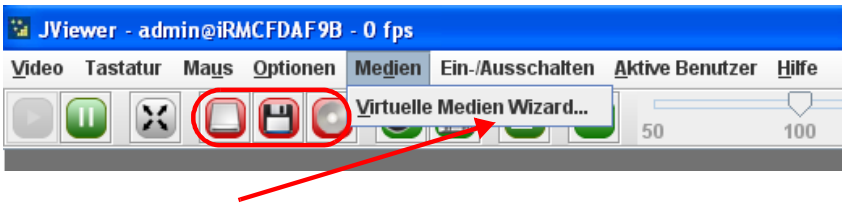



Bild 49: AVR-Fenster - Medien - Virtuelle Medien Wizard...

Der Dialog *Virtuelle Medien* wird geöffnet.

## 6.1.2 Dialog Virtuelle Medien

Je nach den auf der Seite *Virtuelle Medien* der iRMC S4-Weboberfläche vorgenommenen Einstellungen, enthält das Dialogfenster *Virtuelle Medien* zwischen 0 bis hinzu 4 Anzeigen für jeden der folgenden drei Medientypen:

- Floppy-Key Medien (Floppy Images).
  Standard: Kein Floppy Key-Medium wird angezeigt.
- CD/DVD Medien ISO Images.
  - CD/DVD Medien ISO Images
  - CD/DVD-Laufwerke (i.e. physikalische CD/DVD)

  Standard: 2 CD/DVD Medien ISO Images werden angezeigt.
- Festplatte/USB-Key Medien
  - Festplatte/USB Image
  - Physical drive (Festplattenlaufwerk)

  Standard: 1 Festplatte/USB-Key Medium wird angezeigt.

Bei Linux-Systemen müssen physische Speichergeräte gemountet sein.

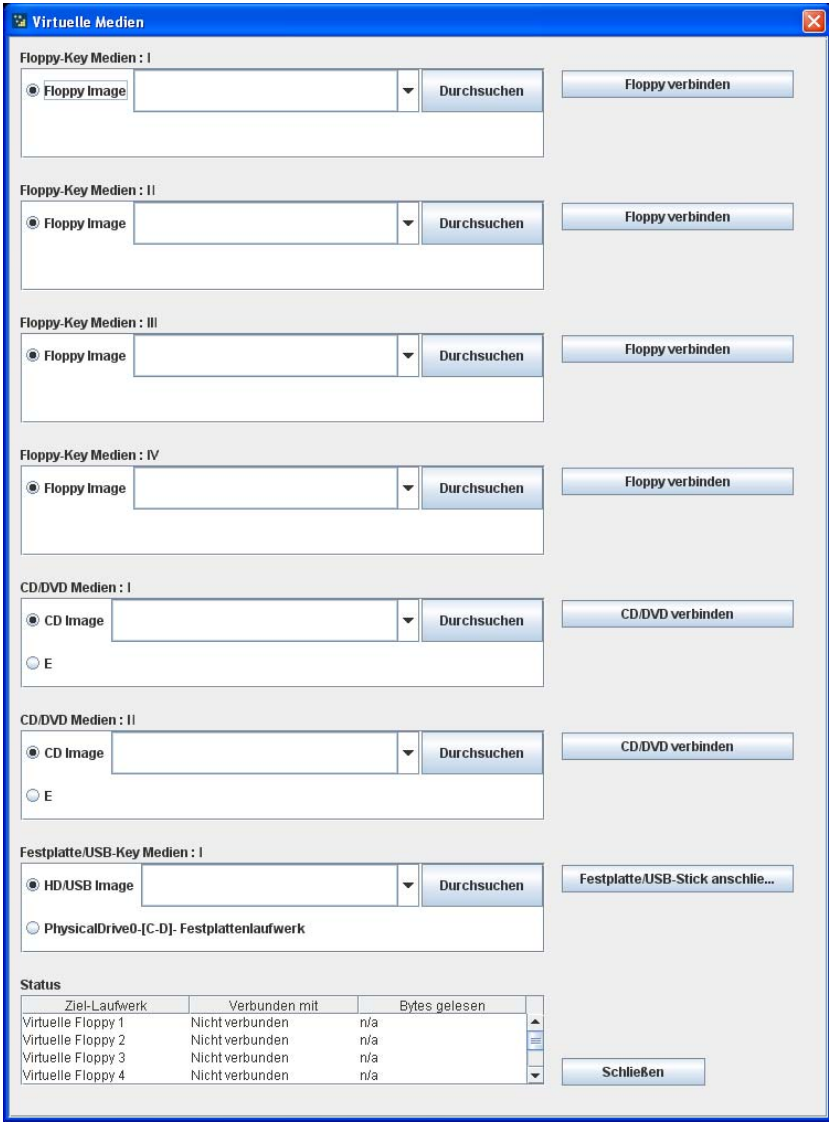



Bild 50: Dialog Virtuelle Medien

Die Anzeige *Status* enthält Informationen zu beiden Speichermedien, die derzeit für virtuelle Medien-Verbindungen verfügbar sind, sowie über die Speichermedien, die derzeit als virtuelle Speichermedien verbunden sind.

### 6.1.3 Speichermedien für virtuelle Medien bereitstellen

Sie können jederzeit während Ihrer AVR-Sitzung die folgenden Aufgaben durchführen:

- Zusätzliche virtuelle Medien-Verbindungen zu den bereits bestehenden hinzufügen
- Einzelne virtuelle Medien-Verbindungen trennen

Gehen Sie folgendermaßen vor, um ein Speichermedium des bevorzugten Typs (z. B. ein DVD-Image) bereitzustellen:

Physikalische Laufwerke werden automatisch angezeigt. Ein Durchsuchen ist nur für die Bereitstellung von Images erforderlich.

- ► Klicken Sie in der entsprechenden Anzeige des Dialogfensters *Virtuelle Medien*auf *Durchsuchen*.

  Das Dateibrowser-Fenster *Öffnen* wird geöffnet.

- ► Navigieren Sie im Dialogfenster *Öffnen* zum Verzeichnis des Speichermediums, das Sie als virtuelles Medium von Ihrer Remote-Workstation aus zur Verfügung stellen möchten.

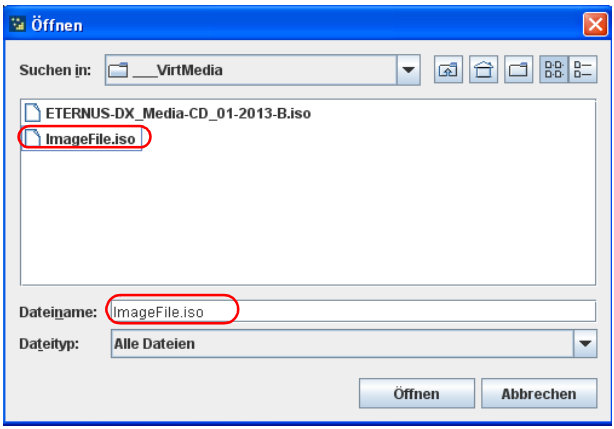



Bild 51: Dialogfenster „Öffnen“ (Windows)

- ► Wählen Sie unter *Dateityp* den erforderlichen Gerätetyp aus.

  Bei Linux-Systemen müssen physische Speichergeräte gemountet sein.

- Geben Sie unter *Dateiname* das Speichermedium an, das Sie als virtuelles Medium verbinden möchten:
  - Bei einem ISO-Abbild (ISO/NRG Image) geben Sie den Dateinamen an. Alternativ klicken auf den im Datei-Browser angezeigten Dateinamen.
  - Bei einem Laufwerk geben Sie den Namen des Laufwerks an, z.B.
    - „D:“ für Laufwerk D (Windows)
    - */dev/...* (Linux)
- Klicken Sie auf *Öffnen*, um Ihre Auswahl zu bestätigen.

  Das ausgewählte Speichermedium wird als virtuelles Medium zur Verfügung gestellt und in der entsprechenden Anzeige des Dialogfensters *Virtuelle Medien* angezeigt.

*Anzeige im Dialog „Remote Storage Geräte“ (Windows)*

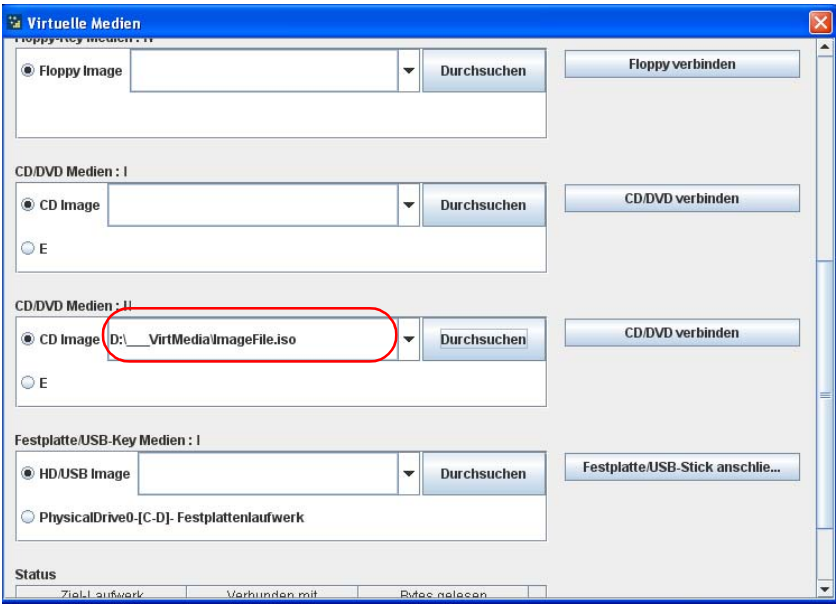



Bild 52: Dialogfenster „Virtuelle Medien“: Das bereitgestellte Speichermedium wird angezeigt.

- Klicken Sie auf die entsprechende Schaltfläche zum *Verbinden*, um das bereitgestellte Speichermedium als virtuelles Medium zu verbinden.

Das ausgewählte Speichermedium wird als virtuelles Medium zur Verfügung gestellt und in der entsprechenden Anzeige des Dialogfensters *Virtuelle Medien* angezeigt.

*Anzeige im Dialog „Remote Storage Geräte“ (Windows)*

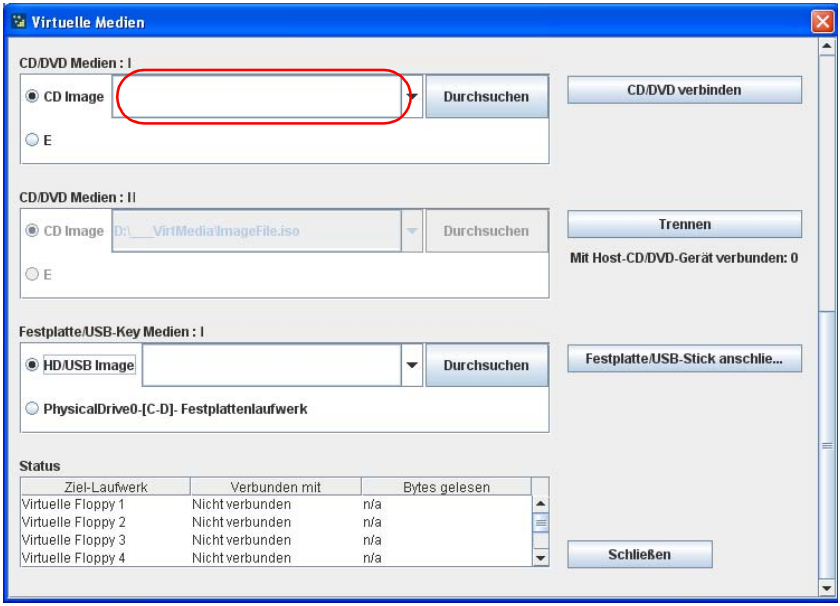



Bild 53: Dialogfenster „Virtuelle Medien“: Das bereitgestellte Speichermedium wird angezeigt.

### 6.1.4 Virtuelle Medien-Verbindungen löschen

In den folgenden Fällen wird eine virtuelle Verbindung automatisch freigegeben:

- Die AVR-Sitzung wird getrennt.
- Die AVR-Sitzung, die die virtuelle Medien-Verbindung hergestellt hat, wechselt aufgrund einer erfolgreichen „Vollzugriff“-Anforderungen einer zweiten AVR-Sitzung in den „Nur Lesen“-Modus.
- Die auf der Seite *Virtual Media Optionen* konfigurierten Einstellungen ändern sich (siehe Seite 357).

► Öffnen Sie das Dialogfenster *Virtuelle Medien* (siehe Abschnitt "Virtuelle Medien Wizard starten" auf Seite 125).

► Führen Sie ein „Sicheres Trennen“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.

► Klicken Sie zum Löschen einer *virtuellen Medien*-Verbindung auf die entsprechende Schaltfläche *Trennen*.

# 7 iRMC-Weboberfläche

Der iRMC verfügt nicht nur über ein eigenes Betriebssystem, sondern fungiert auch als Webserver und bietet eine eigene Weboberfläche. Dabei können Sie wählen, ob Sie sich die Menüs und Dialoge der iRMC-Weboberfläche in deutscher, englischer oder japanischer Sprache anzeigen lassen möchten.

Bei der Eingabe von Werten an der iRMC-Weboberfläche erhalten Sie in vielen Fällen zusätzliche Unterstützung in Form von Tooltips.

Fremd-Lizenzen können angezeigt werden, wenn Sie auf den Link *Lizenzen Dritter* in der Navigationsleiste der iRMC-Weboberfläche klicken (siehe Seite 144).

# 7.1 An der iRMC-Weboberfläche anmelden

► Öffnen Sie am Remote-Arbeitsplatz einen Webbrowser und geben Sie den (konfigurierten) DNS-Namen (siehe Seite 282) oder die IP-Adresse des iRMC ein.

Je nachdem, ob für den iRMC der LDAP-Zugriff auf einen Verzeichnisdienst (Directory Service) konfiguriert ist (Option *LDAP aktiviert*, siehe Seite 314), werden unterschiedliche Anmeldebildschirme angezeigt:

Falls kein Anmeldebildschirm angezeigt wird, überprüfen Sie die LAN-Verbindung (siehe Abschnitt "LAN-Schnittstelle testen" auf Seite 50).

– LDAP-Zugriff des iRMC auf den Verzeichnisdienst ist nicht konfiguriert (Option *LDAP aktiviert* ist nicht aktiviert) und Option *Anmeldung immer aktiv* (siehe Seite 314) ist nicht aktiviert:

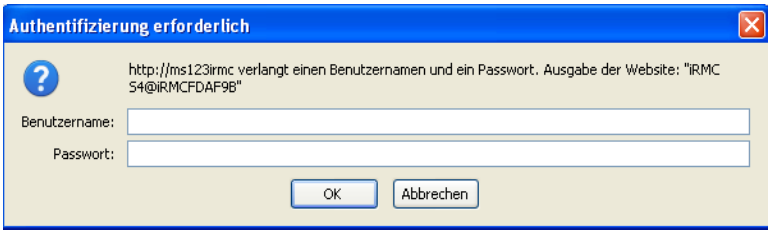



Bild 54: Anmeldebildschirm der iRMC-Weboberfläche (LDAP-Zugriff nicht konfiguriert und Option "SSL Anmeldung immer aktiv" ist nicht gewählt)

► Geben Sie die Daten der Standard-Administratorkennung ein:

*Benutzername*: admin

*Kennwort*: admin

Für *Benutzername* und *Kennwort* wird zwischen Groß- und Kleinschreibung unterschieden.

Aus Sicherheitsgründen wird empfohlen, nach der ersten Anmeldung eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Kennwort zu ändern (siehe "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 302).

► Klicken Sie auf *OK*, um die Einträge zu bestätigen.

– LDAP-Zugriff des iRMC auf den Verzeichnisdienst ist konfiguriert (Option *LDAP aktiviert* ist aktiviert) oder Option *SSL Anmeldung immer aktiv* ist aktiviert):

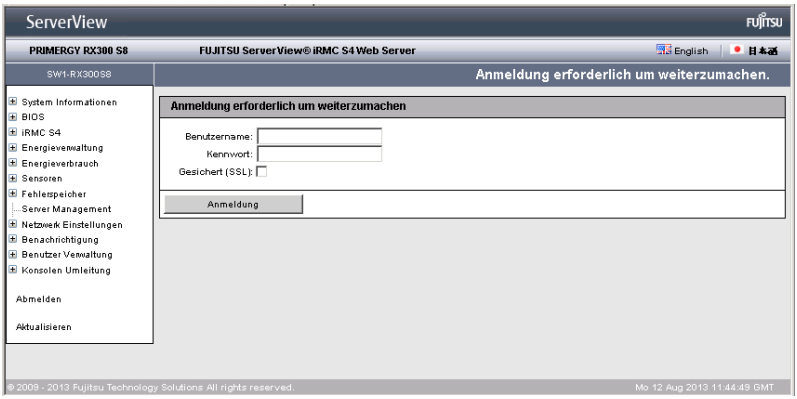



Bild 55: Anmeldebildschirm der iRMC-Weboberfläche (LDAP-Zugriff konfiguriert)

Benutzername und Kennwort werden immer SSL-gesichert übertragen. Wenn Sie die Option *Gesichert (SSL)* aktivieren, erfolgt die gesamte Kommunikation zwischen Webbrowser und iRMC über HTTPS.

► Geben Sie die Daten der Standard-Administratorkennung ein:

*Benutzername*: admin

*Kennwort*: admin

Aus Sicherheitsgründen wird empfohlen, nach der ersten Anmeldung eine neue Administratorkennung anzulegen und die Standard-Administratorkennung zu löschen oder zumindest das Kennwort zu ändern (siehe "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 302).

► Klicken Sie auf *Anmelden*, um die Einträge zu bestätigen.

Die iRMC-Weboberfläche öffnet sich, die Seite *System Information* (siehe Seite 147) wird angezeigt.

# 7.2 Erforderliche Benutzerberechtigungen

Tabelle 5 gibt einen Überblick, welche Berechtigungen zur Nutzung der einzelnen an der iRMC-Weboberfläche angebotenen Funktionen erforderlich sind.

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| **System Information** | | | | | | | | |
| Seite *System Overview* öffnen. | X | X | X | X | | | | |
| Identifizierungs-LED ein-/ausschalten | X | X | X | X | | | | |
| *Inventar Information Konfiguration* setzen. | | | | | | X | | |
| *Betriebssystem Information* editieren[1)] | | | | | | X | | |
| Seite *System Überblick* öffnen. | X | X | X | X | | | | |
| *Fehlerzähler zurücksetzen* | | | | | | X | | |
| *SPD Daten anzeigen*. | X | X | X | X | | | | |
| Seite *AIS Connect* öffnen/bearbeiten. | X | X | | | | | | |
| Seite *SystemReport* öffnen und bearbeiten. | X | X | | | | | | |
| Seite *Netzwerk Übersicht* öffnen. | X | X | X | X | | | | |
| Seite *Driver Monitor* öffnen/bearbeiten. | X | X | X | X | | | | |
| RAID-Information | | | | | | | | |
| Seite *RAID Controller* öffnen.2 | X | X | | | | | | |
| Seite *Festplatten* öffnen.2 | X | X | | | | | | |

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| RAID Physikalisches Laufwerk identifizieren (Schaltfläche*Locate*).2 | X | X | | | | X | | |
| Seite *Festplatten* ansehen.2 | X | X | | | | | | |

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| BIOS | | | | | | | | |
| Seite *BIOS Parameter und Einstellungen sichern/wiederherstellen* öffnen.[1)] | X | X | X | X | | | | |
| *BIOS Parameter und Einstellungen sichern/wiederherstellen* bearbeiten. *Einstellungen*[1)] | X | X | | | | | | |
| Seite *BIOS Einstellungen flashen* öffnen.[1)] | X | X | X | X | | | | |
| BIOS aktualisieren (flashen) [1)] | X | X | | | | | | |
| iRMC S4 | | | | | | | | |
| Seite *iRMC S4 Information* öffnen. | X | X | X | X | | | | |
| *Reboot iRMC S4*. | X | X | | | | | | |
| Lizenzschlüssel (License Key) auf den iRMC S4 laden. | | | | | | X | | |
| *Weitere Optionen* setzen | | | | | | X | | |
| Seite *Save iRMC S4 Time* öffnen. | X | X | X | X | | | | |
| iRMC S4-Zeiteinstellungen ändern. | | | | | | X | | |
| Seite *iRMC S4 FW Einstellungen abspeichern* öffnen. | | | | | X | X | | |
| *Benutzer Einstellungen* wählen. | | | | | X | | | |
| Alle anderen Einstellungen auswählen. | | | | | | X | | |
| iRMC S4 Firmware Einstellungen in WinSCU XML Format importieren | | | | | X | X | | |
| Seite *Zertifikat Austausch* öffnen/bearbeiten. | | | | | | X | | |

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| Seite *Selbstign. RSA Zertifikat erzeugen* öffnen/bearbeiten. | | | | | | X | | |
| Seite *iRMC S4 Aktualisierung* öffnen. | X | X | X | X | | | | |
| Firmware-Selektor setzen | X | X | | | | | | |
| *Firmware Aktualisierung aus einer Datei* ausführen. | X | X | | | | | | |
| Firmware via TFTP aktualisieren (*iRMC S4TFTP...*). | X | X | | | | | | |
| Energieverwaltung | | | | | | | | |
| Seite *Ein-/Ausschalten* öffnen. | X | X | X | X | | | | |
| *Systemstart Optionen* ändern. | | | | | | X | | |
| *Ein-/Ausschalten und Neustart* anwenden. | X | X | X | | | | | |
| Seite *Energieverwaltung Optionen* öffn./bearb. | | | | | | X | | |
| Seite *Netzteil Information* öffnen. | X | X | X | X | | | | |
| Energieverbrauch | | | | | | | | |
| Seite *Konfiguration der Enerergieverbrauchssteuerung* öffnen und bearbeiten. | | | | | | X | | |
| Seite *Akt. System Enerergieverbrauch* öffnen/bearb.[2)] | | | | | | X | | |
| Seite *Energieverbrauch Verlauf* öffnen/bearbeiten[2)]. | | | | | | X | | |
| Sensoren | | | | | | | | |
| Seite *Lüfter* öffnen. | X | X | X | X | | | | |
| Lüfterüberprüf. starten (Gruppe *Lüfter Überprüfung*). | X | X | X | X | | | | |
| *Lüftertest Uhrzeit* setzen (Gruppe *Lüfter Überprüfung*). | | | | | | X | | |

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| Lüftertest aktiviert setzen (Gruppe *System Lüfter*). | | | | | | X | | |
| *Aktion bei Lüfterfehler / Ausschalt Verzögerung* setzen. | | | | | | X | | |
| Seite *Temperatur* öffnen. | X | X | X | X | | | | |
| Aktion bei kritischer Temperatur festlegen. | | | | | | X | | |
| Seite *Spannungen* öffnen. | X | X | X | X | | | | |
| Seite *Netzteil* öffnen. | X | X | X | X | | | | |
| Konfiguration der Stromversorgung Reundanz ausführen. | | | | | | X | | |
| Seite *Komponenten Status* öffnen. | X | X | X | X | | | | |
| Event-Log | | | | | | | | |
| Seite *Fehlerliste* öffnen. | X | X | X | X | | | | |
| Fehlerspeicher löschen. | X | X | X | | | | | |
| *Save event log* (SEL). | X | X | X | X | | | | |
| Fehlergewichte für Fehlerliste festlegen. | X | X | X | X | | | | |
| Seite *Interner Ereignis Speicher Information* öffnen: | X | X | | | | | | |
| Internen Fehlerspeicher (iEL). löschen | X | X | | | | | | |
| *Save event log (iEL).* | X | X | | | | | | |
| Fehlergewichte für Fehlerliste festlegen. | X | X | | | | | | |
| Seite *Fehlerspeicher Konfiguration* öffnen. | X | X | X | X | | | | |
| Standard-Weboberflächen-Anzeigefilter ändern. | | | | | | X | | |

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| SEL-Modus ändern. | | | | | | X | | |
| Service-Desk-Informationen ändern | | | | | | X | | |
| Server Management | | | | | | | | |
| Seite *Server Management Info.* öffnen und bearbeiten. | | | | | | X | | |
| Netzwerkeinstellungen | | | | | | | | |
| Seite *Netzwerk Schnittstelle* öffnen und bearbeiten. | | | | | | X | | |
| Seite *Ports und Netzwerk Dienste* öffnen/bearbeiten. | | | | | | X | | |
| Seite *DNS Konfiguration* öffnen und bearbeiten. | | | | | | X | | |
| Seite *SNMP Konfiguration* öffnen und bearbeiten. | | | | | | X | | |

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| Benachrichtigung | | | | | | | | |
| Seite *SNMP TRAP Benachrichtigung* öffnen und bearb. | | | | | | X | | |
| Seite *E-Mail Benachrichtigung* öffnen und bearbeiten. | | | | | | X | | |
| Benutzerverwaltung | | | | | | | | |
| Seite *iRMC S4 Benutzer* öffnen/bearbeiten. | | | | | X | | | |
| Seite *Verzeichnisdienst Konfiguration* öffnen und bearb. | | | | | | X | | |
| Seite *CAS Konfiguration* öffnen | | | | | X | X | | |
| *CAS Allgemeine Konfiguration* bearbeiten | | | | | | X | | |
| *CAS Benutzer Privileg und Berechtigungen* bearbeiten | | | | | X | | | |
| Konsolen-Umleitung | | | | | | | | |
| Seite *BIOS Text Konsole* öffnen. | X | X | X | X | | | | |
| *BIOS Konsolen Umleitung Optionen* verändern. | | | | | | X | | |
| Text-Konsolen-Umleitung starten | X | X | X | X | | X | | |
| Seite *Graf. Konsolen Umleitung* öffnen und bearbeiten. | | | | | | | X | |
| Virtual Media | | | | | | | | |
| Seite *Virtual Media* öffnen/bearbeiten.[2)] | | | | | | | | X |
| Seite *Dezentrale Medien Abbilder verbinden* öffnen/bearbeiten.[2)] | | | | | | | | X |
| Seite *Media Optionen* öffnen/bearbeiten.[2)] | | | | | | | | X |
| Lifecycle Management | | | | | | | | |

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

| Funktionen an der iRMC-Weboberfläche | Zulässig mit IPMI Privilege Level | | | | Erforderliche iRMC-spezifische Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| Seite *Aktualisierungs Einstellungen* öffnen/bearbeiten. [2] | | | | | | | | X |
| Seite *Online Aktualisierung* öffnen/bearbeiten. | | | | | | | | X |
| Seite *Offline Aktualisierung* öffnen/bearbeiten.[2)] | | | | | | | | X |
| Seite *Custom Image* öffnen/bearbeiten. | | | | | | | | X |
| Seite *PrimeCollect* öffnen/bearbeiten.[2)] | | | | | | | | X |

[1)] Die Aktion ist nur möglich, wenn keine Agenten gestartet sind

[2)] Funktionalität wird nicht von allen PRIMERGY Servern unterstützt.

Tabelle 5: Berechtigungen zur Nutzung der iRMC-Weboberfläche

# 7.3 Aufbau der Bedienoberfläche

Die iRMC-Weboberfläche ist wie folgt aufgebaut:

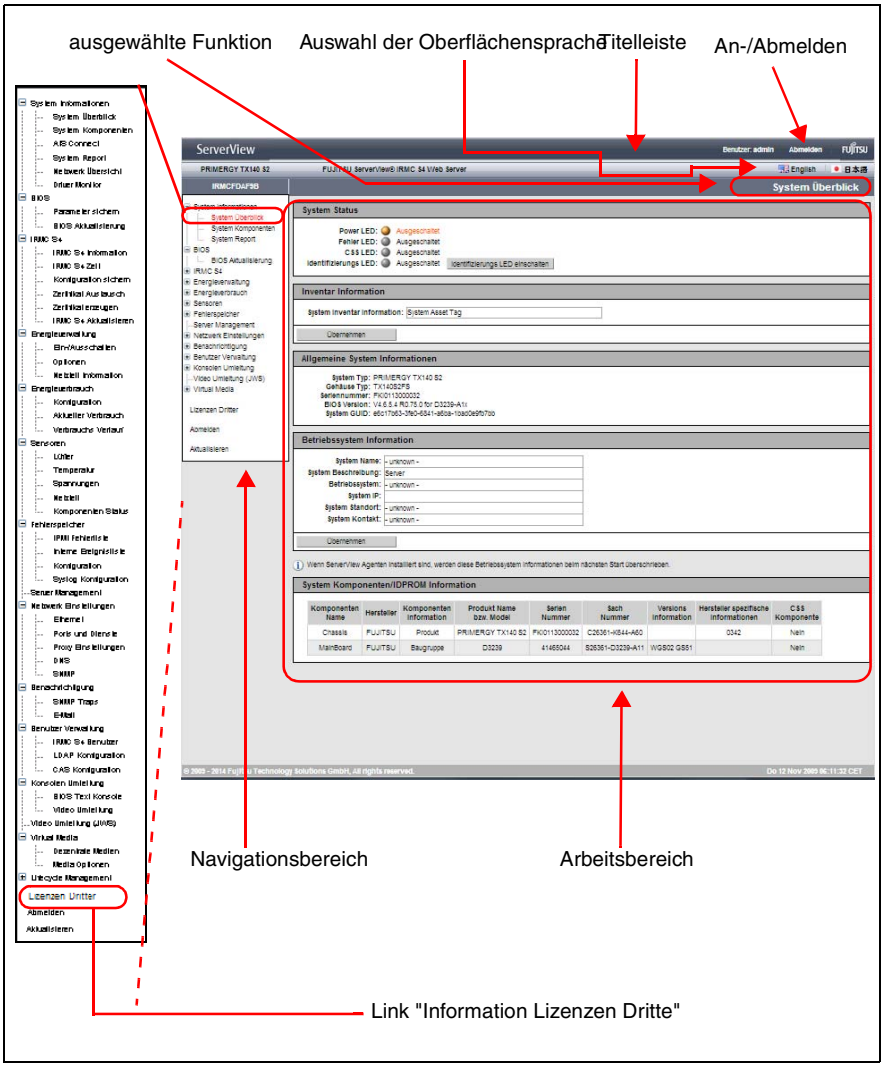



Bild 56: Aufbau der iRMC-Weboberfläche

### Landessprache für die iRMC-Weboberfläche auswählen

In der schwarzen Leiste oberhalb des Arbeitsbereichs finden Sie rechts ein Flaggensymbol. Durch Klicken auf dieses Symbol wählen Sie die Landessprache (Deutsch/Englisch/Japanisch) für die Anzeige von Navigationsbereich, Menüs und Dialogfenstern der iRMC-Weboberfläche.

### Navigationsbereich

Der Navigationsbereich enthält den Menübaum, dessen Knoten die Verweise auf die einzelnen iRMC-Funktionen aufgabenorientiert zusammenfassen. Wenn Sie einen dieser Verweise anklicken, wird der Verweis aktiviert und angezeigt wird der zur Funktion gehörige Arbeitsbereich mit Ausgaben, Dialogfenstern, Optionen, Verweisen und Schaltflächen.

Unterhalb der Verweise zu den einzelnen iRMC-Funktionen finden Sie die Verweise *Abmelden* und *Aktualisieren*:

- Mit *Abmelden* können Sie über einen Bestätigungsdialog die aktuelle iRMC S4-Sitzung beenden. Je nachdem, ob für den iRMC der LDAP-Zugriff auf einen Verzeichnisdienst (Directory Service) konfiguriert ist (Option *LDAP aktiviert*, siehe Seite 314), werden nach Beendigung der Sitzung unterschiedliche Anmelde-Seiten angezeigt:
  - Falls der LDAP-Zugriff des iRMC auf den Verzeichnisdienst nicht konfiguriert ist (Option *LDAP aktiviert* ist nicht aktiviert) und auch die Option *SSL Anmeldung immer aktiv* (siehe Seite 314) deaktiviert ist, wird die folgende Anmelde-Seite angezeigt:

Bild 57: Anmelde-Seite (nach Abmelden)

Durch Klicken auf die Schaltfläche *Anmelden* gelangen Sie zur Anmelde-Seite der iRMC-Weboberfläche, über die Sie sich erneut anmelden können (siehe Bild 54 auf Seite 134). Auf diese Weise können Sie sich erneut anmelden.

– Falls der LDAP-Zugriff des iRMC S4 auf den Verzeichnisdienst konfiguriert ist
(Option *LDAP aktiviert* ist aktiviert) oder die Option *Anmeldung immer aktiv* (siehe Seite 314)aktiviert ist, wird die entsprechende Anmelde-Seite angezeigt (siehe Bild 55 auf Seite 135).

- Mit *Aktualisieren* aktualisieren Sie die Anzeige der iRMC-Weboberfläche.

  Optional können Sie die automatische periodische Aktualisierung der Anzeige konfigurieren (siehe "Automatisch aktualisieren" auf Seite 278).

# 7.4 System Informationen - Informationen zum Server

Der Eintrag *System Informationen* enthält die Verweise auf folgende Seiten:


– "System Überblick - Allgemeine Informationen zum Server" auf Seite 148
– "System Komponenten Information - Informationen zu den Server-Komponenten" auf Seite 154
– "AIS Connect – AIS Connect konfigurieren und verwenden" auf Seite 157
– "System Report" auf Seite 162
– "Netzwerk Anschlüsse" auf Seite 166
– "Driver Monitor" auf Seite 167

## 7.4.1 System Überblick - Allgemeine Informationen zum Server

Die Seite *System Überblick* liefert folgende Informationen:

- System-Status,
- Inventar Information Konfiguration
- System (allgemeine Informationen),
- Betriebssystem des verwalteten Servers,
- Systemkomponenten / IDPROM,
- Gesamt-Energieverbrauch des verwalteten Servers.

Außerdem können Sie auf der Seite *System Überblick* ein von Ihnen gewähltes Bestandskennzeichen („kundenspezifisches Asset Tag“) für den verwalteten Server eintragen.

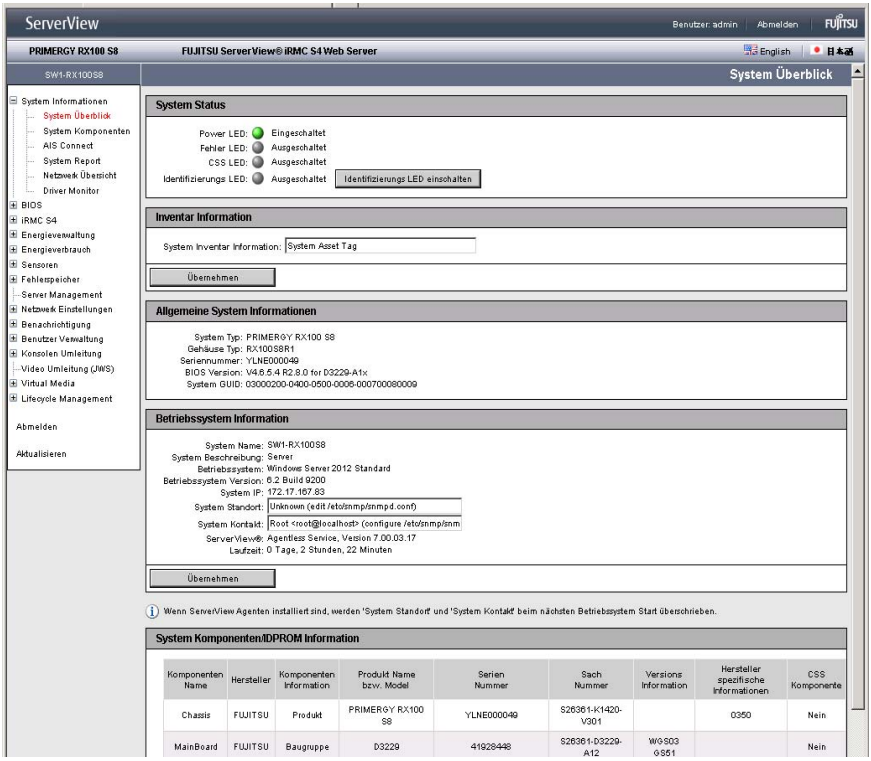


Bild 58: Seite System Überblick

### System Status

Unter *System Status* werden Sie über die CSS-/Globale Fehler-Anzeige am PRIMERGY Server informiert.. Außerdem können Sie die PRIMERGY Identifizierungs-LED ein- und ausschalten.

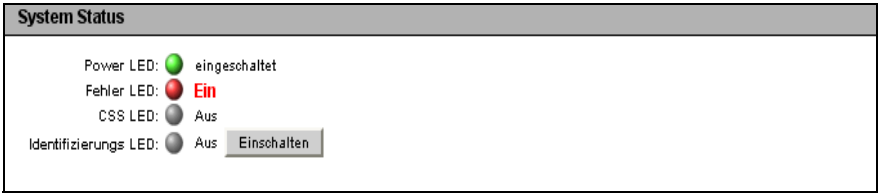



Bild 59: Seite System Überblick - System Status

*Power LED*

Power-Zustand des Servers.
Folgende Status sind möglich:

- Ein: „Power ON“ (grün)
- Aus: „Power OFF“ (orange)

*Fehler LED*

Informiert über Fehler-LED (Global Error-LED) am Server:

| Anzeige (iRMC) | Global Error LED am Server | Systemstatus |
|---|---|---|
| Aus | Leuchtet nicht | Es liegt kein kritisches Ereignis vor. |
| Ein | Leuchtet rot | Prefailure-Ereignis für eine Nicht-CSS-Komponente. |
| Blinkend | Blinkt rot. | Kritisches Ereignis. |

*CSS LED*

Informiert über CSS (Customer Self Service)-LED am Server:

| Anzeige (iRMC) | CSS-LED am Server | Systemstatus |
|---|---|---|
| Aus | Leuchtet nicht | Der Server ist in Ordnung. |
| Ein | Leuchtet orange. | Prefailure-Ereignis für eine CSS-Komponente. |
| Blinkend | Blinkt orange. | Defekte CSS-Komponente. |

*Identifizierungs LED*

Identifizierung des Servers.
Folgende Status sind möglich:

– eingeschaltet (blau)
– ausgeschaltet: (grau)

*Einschalten / Ausschalten*

Durch Klicken auf die alternierende Schaltfläche *Einschalten / Ausschalten* können Sie die Identifizierungs-LED ein- bzw. ausschalten.

### Inventar Information Konfiguration

Unter *Inventar Information Konfiguration* können Sie ein von Ihnen gewähltes Bestandskennzeichen („kundenspezifisches Asset Tag“) für den verwalteten Server eintragen.

Mithilfe des kundspezifische Asset Tags können Sie dem Server eine von Ihnen gewählte Inventarnummer oder sonstige Identifikation geben.

Bei Windows-basierten Systemen wird das kundenspezifische Asset Tag automatisch von der WMI (Windows Management Instrumentation) bereitgestellt. Es kann dann mithilfe von internen Tools ausgewertet werden oder für die Integration in Unternehmens-Managementsysteme (wie CA Unicenter) verwendet werden.

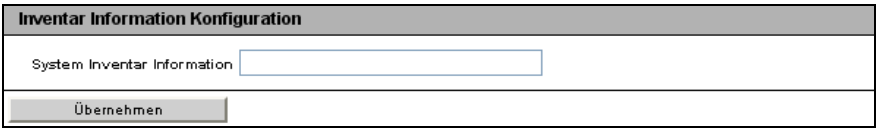



Bild 60: Seite System Überblick – Inventar Information Konfiguration

*Sytem Inventar Information*

Hier können Sie das Bestandskennzeichen eingeben.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um das Bestandskennzeichen zu übernehmen.

### Allgemeine System Informationen

Unter *Allgemeine Sytem Informationen* sind Informationen zum verwalteten Server aufgelistet.

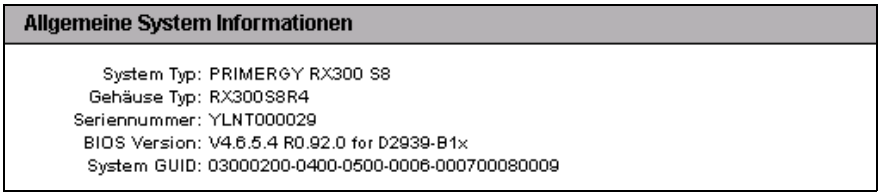



Bild 61: Seite System Überblick Allgemeine System Informationen

### Betriebssystem Information

Unter *Betriebssystem Information* werden Informationen zum Betriebssystem des verwalteten Servers aufgelistet und es wird angezeigt, ob die ServerView Agents auf dem verwalteten Server verfügbar sind oder ob der ServerView Agentless Service auf dem verwalteten Server verfügbar ist.

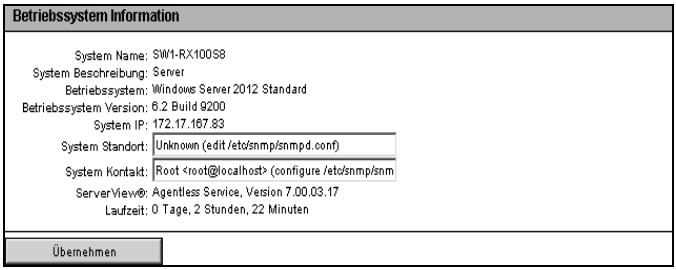

Betriebssystem Information
System Name: SW1-RX100S8
System Beschreibung: Server
Betriebssystem: Windows Server 2012 Standard
Betriebssystem Version: 6.2 Build 9200
System IP: 172.17.167.83
System Standort: Unknown (edit /etc/snmp/snmpd.conf)
System Kontakt: Root <root@localhost> (configure /etc/snmp/snm
ServerView®: Agentless Service, Version 7.00.03.17
Laufzeit: 0 Tage, 2 Stunden, 22 Minuten
Übernehmen

Bild 62: Seite System Überblick - Betriebssystem Information

Wenn weder ein ServerView-Agent noch der ServerView Agentless Service ausgeführt wird, können Sie alle Felder der Gruppe *Betriebssystem Information* bearbeiten. Andernfalls sind diese Felder nicht bearbeitbar.

Wenn die ServerView Agents ausgeführt werden, werden alle Werte von den ServerView Agents festgelegt. Die Werte können manuell angepasst werden, jedoch nur "in band".

Wenn der ServerView Agentless Service ausgeführt wird, werden alle Werte, außer den Werten für *System Standort* und *System Kontakt*, festgelegt. Auf diese Werte kann der ServerView Agentless Service nicht zugreifen. Die Werte für *System Standort* und *System Kontakt* können manuell festgelegt werden.

### System Komponenten/IDPROM Information

Unter *Sytem Komponenten/IDPROM Information* sind Informationen zu den FRUs (**F**ield **R**eplaceable **U**nits) aufgelistet. FRUs sind Systemkomponenten, die freigegeben und aus dem System entfernt werden können. In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice) -Funktionalität unterstützt wird.

**System Komponenten/IDPROM Information**

| Komponenten Name | Hersteller | Komponenten Information | Produkt Name bzw. Model | Serien Nummer | Sach Nummer | Versions Information | Hersteller spezifische Informationen | CSS Komponente |
|---|---|---|---|---|---|---|---|---|
| Chassis | FUJITSU | Produkt | PRIMERGY RX300 S8 | YLNT000029 | S26361-K1457-V201 | | 0356 | Nein |
| MainBoard | FUJITSU | Baugruppe | D2939 | 40841429 | S26361-D2939-E17 | WGS08 GS52 | | Nein |
| PSU1 | DELTA | Baugruppe | DPS-800NB A | DCOD1222032059 | A3C40121107 | S6F | | Ja |
| PSU2 | DELTA | Baugruppe | DPS-800NB A | DCOD1222032134 | A3C40121107 | S6F | | Ja |

Bild 63: Seite System Überblick - System Komponenten/IDPROM Information

### Aktueller Gesamt Energieverbrauch

Diese Option wird nicht für alle PRIMERGY Server unterstützt.

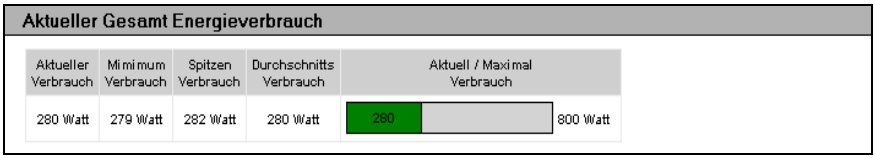



Bild 64: Seite System Überblick Aktueller Gesamt Energieverbrauch

Unter *Aktueller Gesamt Energieverbrauch* werden die Messwerte zum aktuellen, minimalen, maximalen sowie durchschnittlichen Energieverbrauch des verwalteten Servers im aktuellen Intervall angezeigt.

In einer grafischen Anzeige wird außerdem der aktuelle Energieverbrauch des Servers der maximal möglichen Leistungsaufnahme gegenübergestellt.

## 7.4.2 System Komponenten Information - Informationen zu den Server-Komponenten

Die Seite *System Komponenten Information* liefert Informationen zur CPU und den Hauptspeicher-Modulen. In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice) -Funktionalität unterstützt wird.

Die möglichen Status der Systemkomponenten werden durch folgende Status-Icons symbolisiert:

| | |
|---|---|
| | OK: Der Zustand der Komponente ist in Ordnung. |
| | Der Steckplatz für die Komponente ist leer. |
| | Warnung: Der Zustand der Komponente hat sich verschlechtert. |
| | Fehler: Die Komponente hat einen Fehler. |

Tabelle 6: Status der Systemkomponente

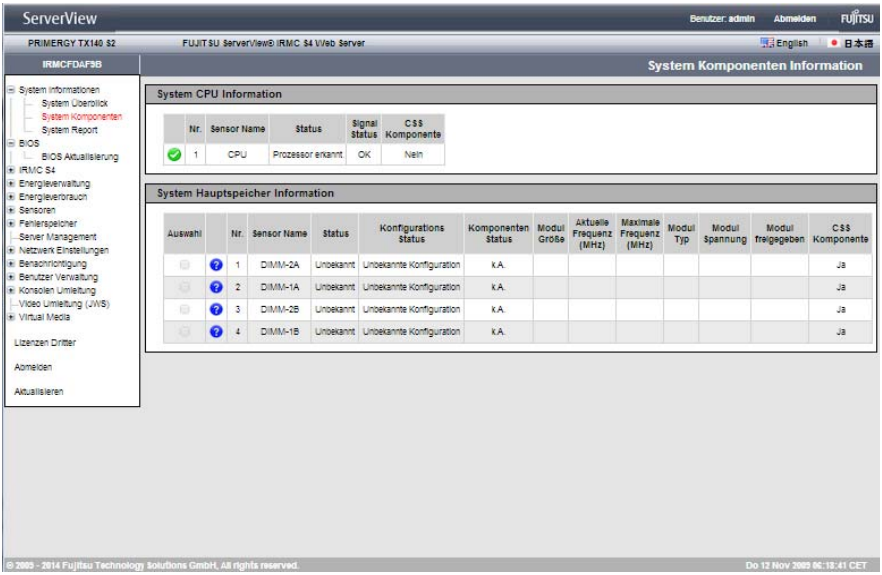



Bild 65: Seite System Komponenten Information (ohne SPD-Daten)

Bei PRIMERGY Servern mit TPM (Trusted Platform Module)-Unterstützung wird angezeigt, ob TPM aktiviert oder deaktiviert ist.

### System CPU Information

Diese Gruppe informiert unter anderem über Status, IDs, CSS-Fähigkeit und Leistung der CPU(s) im verwalteten PRIMERGY Server.

### System Hauptspeicher Information

Diese Gruppe informiert über Status, IDs, CSS-Eignung und Leistungsdaten der Hauptspeichermodule im verwalteten PRIMERGY Server.

*Auswahl*
Hier können Sie einzelne Speichermodule auswählen, auf die die unter *Wählen Sie eine Aktion aus der Liste* ausgeführt werden soll.

*Alle auswählen*
Wählt alle Speichermodule aus.

*Auswahl löschen*
Löscht die Auswahl.

*Wählen Sie eine Aktion aus der Liste*
In dieser Liste, die nur bei einem Fehler angezeigt wird, können Sie eine Aktion auswählen, die für die ausgewählten Speichermodule angewendet wird.

Die folgenden Aktionen stehen zur Auswahl bereit:

*Reset Error Counter*
Setzt den Fehlerzähler zurück.

Bei einem iRMC oder Server Blade muss der Fehlerzähler nicht mehr ausdrücklich zurückgesetzt werden, da neue Module automatisch erkannt werden, wenn der Fehlerzähler auf 0 gesetzt ist.

*Für ausgewählte Module übernehmen*
Aktiviert das Speichermodul.

*Für ausgewählte Module übernehmen*
Führt die gewählte Aktion auf die ausgewählten Speichermodule aus.

*SPD Daten anzeigen / Keine SPD Daten anzeigen*
Durch Klicken auf die alternierende Schaltfläche *SPD Daten anzeigen / Keine SPD Daten anzeigen* blenden Sie Hersteller-spezifische Angaben (**S**erial **P**resence **D**etect (SPD)-Daten) zu den einzelnen Speicherkomponenten ein- bzw. aus.

Die SPD-Daten einer Speicherkomponente sind auf einem in die Komponente integrierten EEPROM abgelegt und dienen der automatischen Erkennung dieser Speicherkomponente (RAM, DIMM) durch das BIOS.

### 7.4.3 AIS Connect – AIS Connect konfigurieren und verwenden

Auf der Seite *AIS Connect* können Sie die eingebettete AIS Connect-Funktion des iRMC konfigurieren.

Mithilfe von AIS Connect (AutoImmuneSystems©) kann ein PRIMERGY Server dezentral überwacht und in einigen Fällen auch über das Servicesystem von Fujitsu Technology Solutions gesteuert werden. In diesem Fall steuert ein Servicetechniker den weiteren Workflow.

Die AIS Connect-Funktion ermöglicht Folgendes:

– Zulassen, dass der eingebettete AIS-Agent des iRMC automatische Aufrufe an den technischen Support von Fujitsu Technology Solutions sendet.

– Zulassen, dass der technische Support von Fujitsu Technology Solutions PrimeCollect-Archive vom iRMC abruft.

– Zulassen, dass der technische Support von Fujitsu Technology Solutions Systemberichtsdaten vom iRMC abruft.

– Zulassen, dass der technische Support von Fujitsu Technology Solutions eine Verbindung zur iRMC-Weboberfläche des iRMC herstellt.

Für das Senden von PrimeCollect-Archiven ist ein gültiger eLCM-Lizenzschlüssel erforderlich (siehe "Lizenz Schlüssel (License Key)" auf Seite 193).

AIS Connect stellt eine Verbindung zwischen dem eingebetteten AIS Connect-Client (AIS-Agent) auf dem iRMC S4 und dem Servicesystem von Fujitsu Technology Solutions her. Über diese Verbindung kann ein Techniker von einem dezentralen Ort selbst dann auf den iRMC S4 zugreifen, wenn kein direkter LAN-Zugriff auf den iRMC S4 möglich ist. Falls ein Fehler auftritt, werden Systeminformationen (PrimeCollect-Archive, Systemberichte usw.) auf diesem Weg übertragen.

Für die eingebettete AIS Connect-Funktion stehen zwei verschiedene Modi zur Auswahl:

– *Garantiemodus*

  Im *Garantiemodus* besteht die einzige Funktion von AIS Connect darin, die Unternehmensumgebung (das Servicesystem) auf täglicher Basis zu kontaktieren und von Prime Collect erstellte Daten nur nach entsprechender Aufforderung des Benutzers zu senden.

– *Vertragsmodus*

  Im *Vertragsmodus* meldet AIS Connect alle Probleme, die während des Serverbetriebs auftreten. Neben den Alarmdaten werden auch PrimeCollect- und SystemReport-Berichte gesendet.

*Garantiemodus* ist die Standardauswahl. Nur die Techniker, die die Unternehmensumgebung verwalten, können einen Wechsel vom *Garantiemodus* in den *Vertragsmodus* vornehmen. Hierfür muss eine Verbindung eingerichtet werden.

Die Verwendung der eingebetteten AIS Connect-Funktion des iRMC wird weiter unten beschrieben. Ausführliche Informationen zur eingebetteten AIS-Funktion erhalten Sie im Handbuch "ServerView embedded Lifecycle Management (eLCM)".

Alternativ können Sie die generierte XML-Datei mithilfe eines cURL- oder Visual Basic-Skripts herunterladen und automatisch bewerten (siehe Abschnitt "Download per Skript und automatische Bewertung des iRMC S4-Reports" auf Seite 496 ).

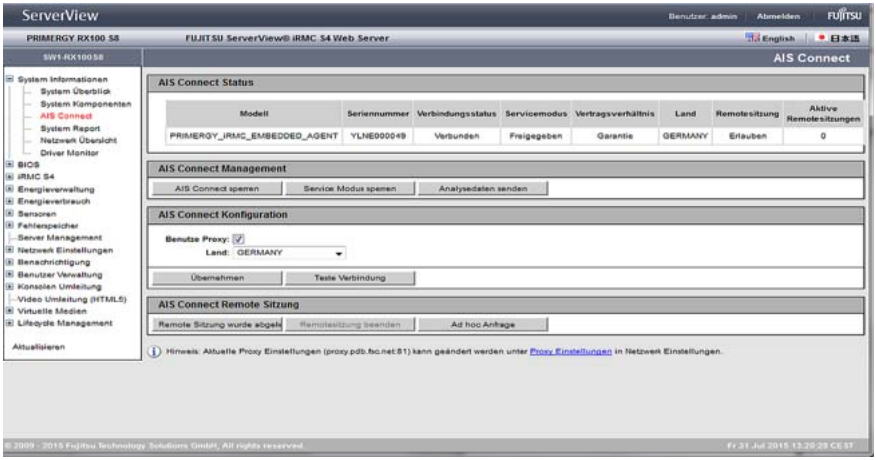



Bild 66: Seite "AIS Connect"

### AIS Connect Status

Die Gruppe *AIS Connect Status* enthält Informationen zum Status des eingebetteten AIS-Agenten. Der Wert "PRIMERGY iRMC EMBEDDED AGENT" bei *Modell* ist für alle PRIMERGY Server vorgegeben. *Vertragsverhältnis* zeigt den Modus an, in dem AIS Connect aktuell ausgeführt wird (*Garantiemodus* oder *Vertragsmodus*). Die anderen Werte, die in der Gruppe *AIS Connect Status* angezeigt werden, hängen von den Aktionen und Werten ab, die auf der Seite *AIS Connect* gestartet bzw. konfiguriert wurden.

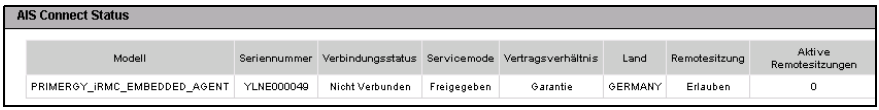



Bild 67: Seite "AIS Connect" – AIS Connect Status

### AIS Connect Management

In der Gruppe *AIS Connect Management* können Sie AIS Connect aktivieren/deaktivieren. Wenn sich AIS Connect aktuell im *Vertragsmodus* befindet, können Sie den eingebetteten AIS Connect-Agenten auch in den Servicemodus schalten. In diesem Modus ignoriert der Agent alle von Hardware ausgelösten Alarme.

Bild 68: Seite "AIS Connect" – AIS Connect Management

*AIS Connect freigeben/AIS Connect deaktivieren*
: Aktiviert/deaktiviert AIS Connect.

*Servicemode freigeben/Servicemode deaktivieren*
: Aktiviert/deaktiviert den Servicemodus.

*Analysedaten senden*
: Sendet die AIS Connect-Analysedatei an den technischen Support von Fujitsu Technology Solutions.

### AIS Connect Konfiguration

In der Gruppe *AIS Connect Konfiguration* können Sie die AIS Connect-Einstellungen konfigurieren.

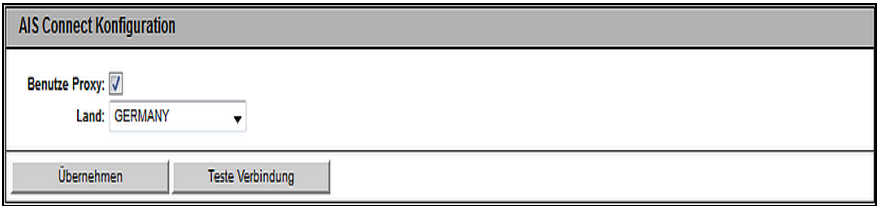



Bild 69: Seite "AIS Connect" – AIS Connect Konfiguration

*Benutze Proxy*

Hier können Sie auswählen, ob ein HTTP-Proxyserver verwendet werden soll. Die Proxyserver-Einstellungen können auf der Seite *Proxy Einstellungen* unter *Netzwerk Einstellungen* konfiguriert werden (siehe Abschnitt "Proxy Einstellungen– Proxyeinstellungen konfigurieren" auf Seite 280).

*Land*

AIS Connect RP Land.

*Übernehmen*

Aktiviert Ihre Einstellungen.

Wenn Sie auf *Übernehmen* klicken, werden die Einstellungen im persistenten Speicher des iRMC gespeichert. Die Einstellungen sind deshalb weiterhin verfügbar, nachdem eine Seite aktualisiert wurde, nachdem die iRMC-Weboberfläche geschlossen und wieder geöffnet wurde oder wenn ein Stromausfall aufgetreten ist.

*Teste Verbindung*

Testet die Verbindung zum Service-System von Fujitsu Technology Solutions.

### AIS Connect Remote Sitzung

In der Gruppe *AIS Connect Remote Sitzung* können Sie folgende Vorgänge ausführen:

– Policy für die Remote-Sitzung aktivieren oder deaktivieren.

– Remote-Sitzungen trennen.

– Sofortigen Abruf durch den eingebetteten AIS Connect-Agenten erzwingen. Dies ist nützlich, um im *Garantiemodus* eine schnelle Antwort zu erhalten.

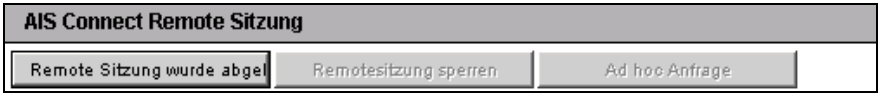



Bild 70: Seite "AIS Connect" – AIS Connect Konfiguration

*Remotesitzung erlauben/Remote Sitzung wurde abgelehnt*

Erlaubt/verweigert eine Remote-Sitzung durch die Aktivierung/Deaktivierung der Policy für die Remote-Sitzung.

*Remotesitzung sperren*

Trennt eine gegebenenfalls bestehende Remote-Sitzung.

*Ad hoc Anfrage*

Erzwingt einen sofortigen Abruf durch den eingebetteten AIS Connect-Agenten.

## 7.4.4 System Report

The *System Report* page provides information on service incidents concerning server hardware/software directly out-of-band from the iRMC.

Es werden Informationen zu den folgenden Elementen bereitgestellt:

- BIOS
- Processor
- Memory
- Temperatur-Sensoren
- Stromversorgungen
- Spannungssensoren
- IDPROMS
- PCI-Geräte
- Fehlerspeicher
- Interner Ereignisspeicher
- Boot-Status
- Management-Controller

Alternativ können Sie die generierte XML-Datei mithilfe eines cURL- oder Visual Basic-Skripts herunterladen und automatisch bewerten (sieheAbschnitt "Download per Skript und automatische Bewertung des iRMC S4-Reports" auf Seite 496).

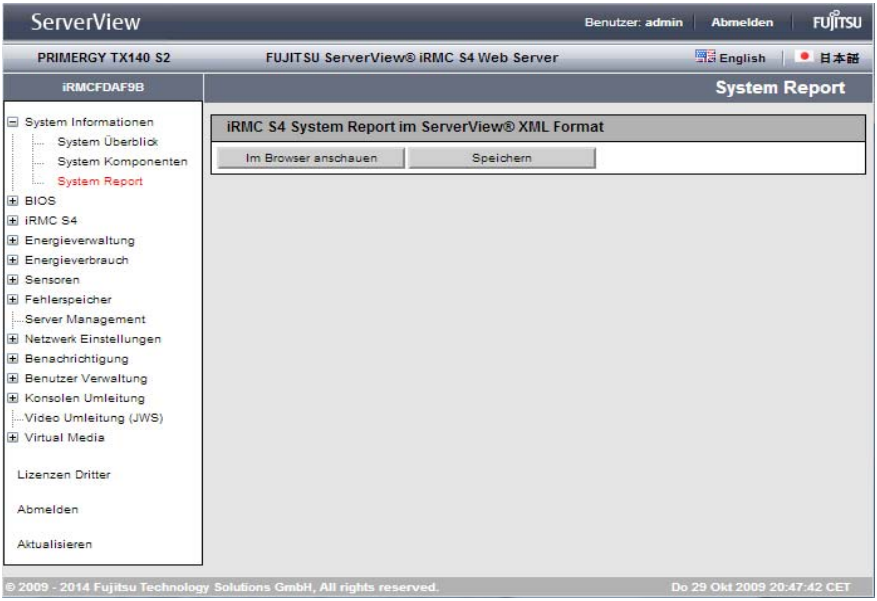


Bild 71: Seite "System Report"

*Im Browser anschauen*

Zeigt die XML-Datei an, die die Berichtsinformationen enthält.

*Speichern*

Speichert eine Datei *report.xml* mit den Berichtsinformationen im lokalen Download-Verzeichnis. Für jede gespeicherte Berichtsdatei wird eine Schaltfläche *report.xml* am unteren Rand der Seite *System Report* angezeigt. Durch Klicken auf die entsprechende Schaltfläche können Sie eine Berichtsdatei öffnen.

Mithilfe der Datei *PcSysScan.exe* auf der ServerView Suite-DVD 2 können Sie die generierte XML-Datei folgendermaßen in eine von Menschen lesbare HTML-Datei transformieren:

```
PcSysScan.exe -xmltransform report.xml report.html
```

## 7.4.5 CPU-Auslastungs-Historie

Die Funktion CPU-Auslastung stellt eine Datenanalyse der gesamten CPU-Nutzung über einen ausgewählten Zeitraum zur Verfügung.

Die gesammelten Daten werden in einem Diagramm angezeigt, das die maximalen, die minimalen und die durchschnittlichen Werte der CPU-Auslastung für ein einzelnes Beispiel oder für alle Beispiele im gesamten ausgewählten Zeitraum enthält.

Die Funktion CPU-Auslastung sammelt nur dann reale Datenbeispiele, wenn der Host-Rechner an ist.

Wenn der Host-Rechner aus ist, werden Daten simuliert. (Alle 30 Sekunden werden fingierte Beispiele mit Wert 0 generiert).

Die Funktion CPU-Auslastung ist nur für Systeme verfügbar, auf denen der Node Manager die CUPS-Funktionalität unterstützt (NM_SENS_CORE_CPUS).

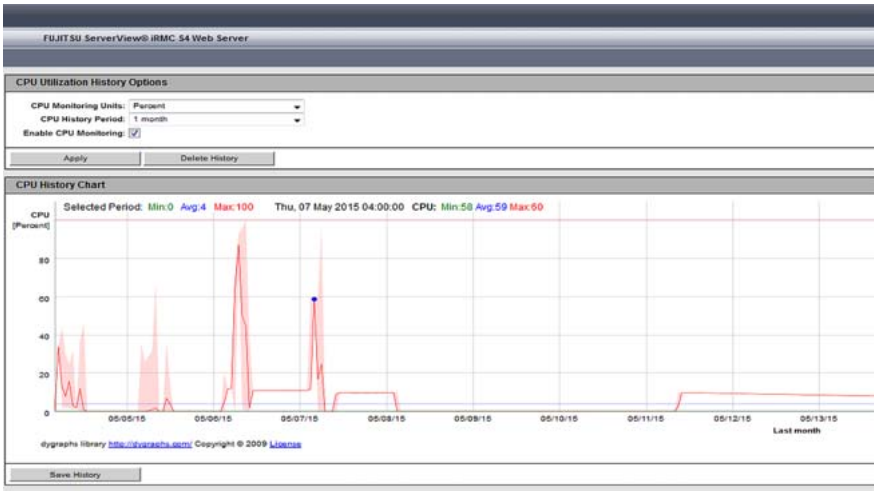



Bild 72: Seite CPU-Auslastungs-Historie

### CPU-Auslastungs-Historie - Optionen

Unter *CPU Utilization History Options* können Sie die Einstellungen für die Diagrammansicht ändern.

*CPU Monitoring Units*
: Einheit der CPU-Auslastung

*CPU History period*
: Auswählbarer Zeitraum zwischen einer Stunde und fünf Jahren. Beispiele für eine Stunde, zwölf Stunden und einen Tag sind temporär und werden nicht gespeichert. Beispiele für eine Woche, zwei Wochen, einen Monat, ein Jahr und fünf Jahre werden im Flash-Speicher gespeichert (dateibasiert). Beispiele für eine Woche, zwei Wochen und einen Monat werden stündlich gespeichert. Beispiele für ein Jahr und fünf Jahre werden gespeichert.

*Enable CPU monitoring*
: Aktiviert die Überwachung in dem definierten Zeitraum.

*Übernehmen*
: Wendet die ausgewählten Optionen an.

*Delete History*
: Löscht die gesammelten Daten.

### CPU History Chart

Zeigt die gesammelten Daten in einem Diagramm mit der Einheit als x-Achse und dem Zeitraum als y-Achse.

*Save History*
: Öffnet einen Dialog zur Auswahl des Verzeichnisses, in dem die gesammelten Daten gespeichert werden.

## 7.4.6 Netzwerk Anschlüsse

Die *Seite Netzwerk Anschlüsse* enthält Informationen zu den Ethernet-Ports des iRMC.

Bild 73: Seite „Netzwerk Anschlüsse“

## 7.4.7 Driver Monitor

Die Seite *Driver Monitor* enthält Informationen zu den auf dem System installierten Treibern.

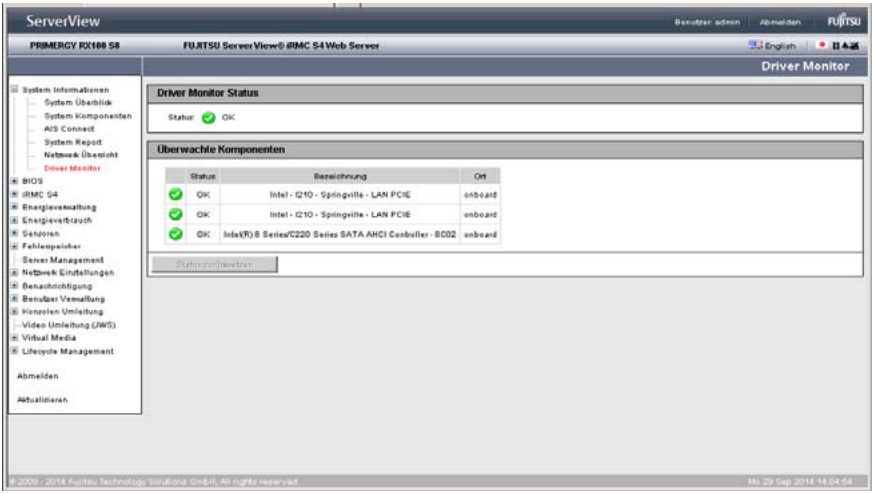



Bild 74: Seite "Driver Monitor"

*Driver Monitor Status*
: Zeigt den allgemeinen Überwachungsstatus der Treiber an.

*Überwachte Komponenten*
: Zeigt die überwachten Treiberkomponenten an.

*Neustart*
: Setzt den Status aller Treiberkomponenten zurück.

# 7.5 RAID Informationen - Informationen zu den RAID-Systemen

Der Eintrag *RAID Informationen* und die entsprechenden Seiten werden nur angezeigt, wenn die folgenden Anforderungen erfüllt sind:

- Auf dem verwalteten Server stehen Out-of-Band-fähige RAID Controller zur Verfügung
- Der Server ist eingeschaltet und das System befindet sich derzeit nicht in der BIOS POST-Phase.

Der Eintrag *RAID Informationen* enthält Links zu den folgenden Seiten:

- "RAID Controller - Informationen zu RAID Controllern und verbundenen Batterien" auf Seite 169
- "Festplatteneinheiten – Informationen zu RAID-Festplatteneinheiten" auf Seite 171
- "Festplatten - Informationen zu RAID Physikalische Laufwerke" auf Seite 175
- "Logische Laufwerke - Informationen über logische RAID-Laufwerke" auf Seite 177

Diese Seiten, die nachfolgend detailliert beschrieben werden, enthalten nur Informationen zu RAID-Systemen. Zum Verwalten von RAID-Systemen ist weiterhin ServerView RAID erforderlich.

## 7.5.1 RAID Controller - Informationen zu RAID Controllern und verbundenen Batterien

Die Seite *RAID Controller* enthält für jeden RAID Controller auf dem verwalteten Server entsprechende Informationen sowie Angaben zum Status der verbundenen Batterie.

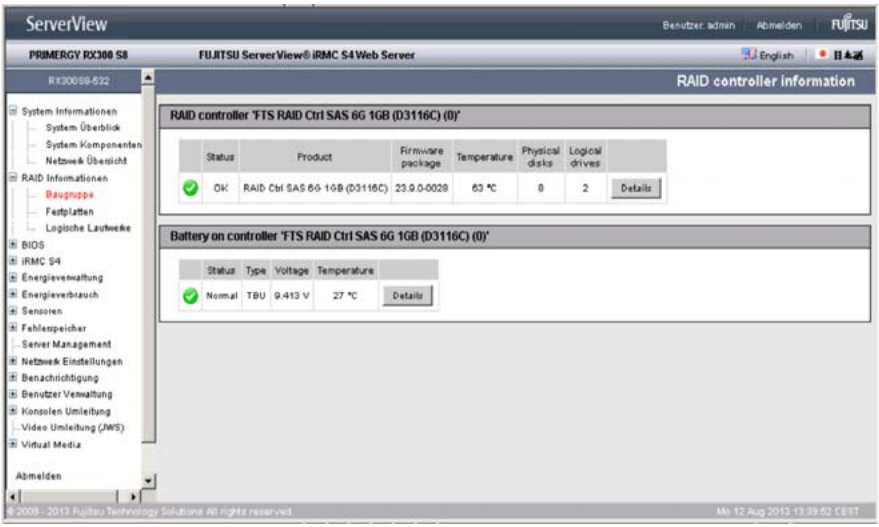



Bild 75: RAID Informationen - Seite „Controller“

*Details*

Durch Klicken auf *Details* wird eine neue Seite geöffnet, die detaillierte Informationen zum RAID Controller bzw. zur Batterie enthält.

Bild 76: Details zum RAID Controller

## 7.5.2 Festplatteneinheiten – Informationen zu RAID-Festplatteneinheiten

Die Seite *RAID Festplatteneinheit Information* enthält Informationen zu jeder RAID-Festplatteneinheit des verwalteten Servers.

### RAID-Festplatteneinheit: ETERNUS JX40

Bild 77: RAID Informationen – Seite für RAID-Festplatteneinheiten (ETERNUS JX40)

*Einzelheiten*

Durch Klicken auf *Einzelheiten* wird eine neue Seite geöffnet, die detaillierte Informationen zur entsprechenden RAID-Festplatteneinheit enthält.

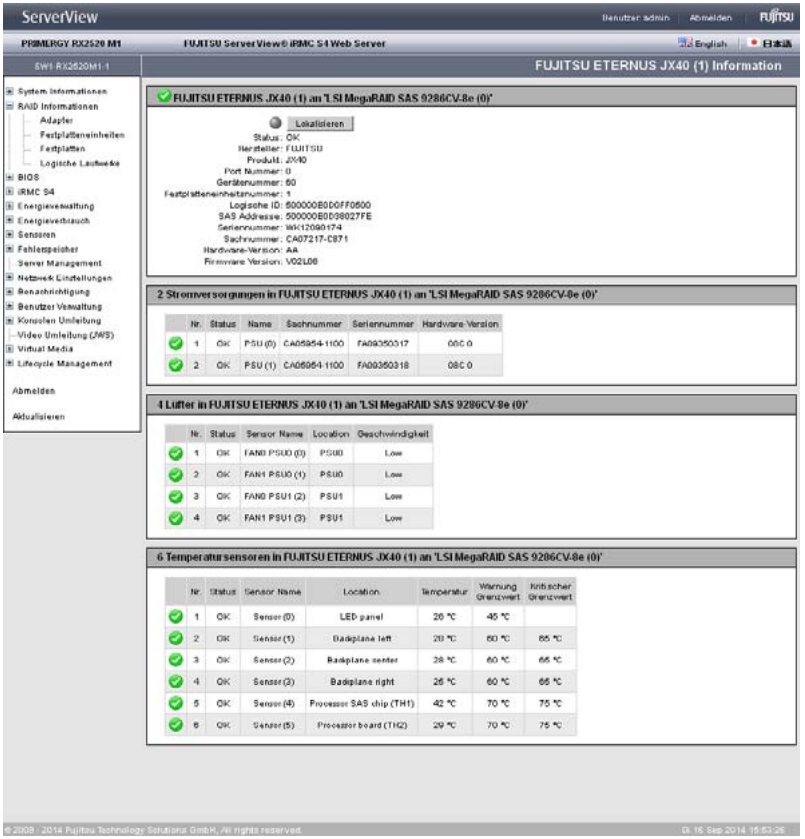

ServerView
Benutzer: admin
Abmelden
FUJITSU
PRIMERGY RX2520 M1
FUJITSU ServerView® iRMC S4 Web Server
English
日本語
FUJITSU ETERNUS JX40 (1) Information
System Informationen
RAID Informationen
Adapter
Festplatteneinheiten
Festplatten
Logische Laufwerke
BIOS
iRMC S4
Energieverwaltung
Energieverbrauch
Sensoren
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigung
Benutzer Verwaltung
Konsolen Umleitung
Video Umleitung (JWS)
Virtual Media
Lifecycle Management
Abmelden
Aktualisieren
FUJITSU ETERNUS JX40 (1) an 'LSI MegaRAID SAS 9286CV-8e (0)'
Lokalisieren
Status: OK
Hersteller: FUJITSU
Produkt: JX40
Port Nummer: 0
Gerätenummer: 60
Festplatteneinheitsnummer: 1
Logische ID: 600000E0D0FF0600
SAS Address: 5000000E0D38027FE
Seriennummer: WK12090174
Sachnummer: CA07217-C871
Hardware-Version: AA
Firmware Version: V02L00
2 Stromversorgungen in FUJITSU ETERNUS JX40 (1) an 'LSI MegaRAID SAS 9286CV-8e (0)'
Nr. Status Name Sachnummer Seriennummer Hardware-Version
1 OK PSU (0) CA05954-1100 FA09350317 08C 0
2 OK PSU (1) CA05954-1100 FA09350318 08C 0
4 Lüfter in FUJITSU ETERNUS JX40 (1) an 'LSI MegaRAID SAS 9286CV-8e (0)'
Nr. Status Sensor Name Location Geschwindigkeit
1 OK FAN0 PSU0 (0) PSU0 Low
2 OK FAN1 PSU0 (1) PSU0 Low
3 OK FAN0 PSU1 (2) PSU1 Low
4 OK FAN1 PSU1 (3) PSU1 Low
6 Temperatursensoren in FUJITSU ETERNUS JX40 (1) an 'LSI MegaRAID SAS 9286CV-8e (0)'
Nr. Status Sensor Name Location Temperatur Warnung Grenzwert Kritischer Grenzwert
1 OK Sensor (0) LED panel 26 °C 45 °C
2 OK Sensor (1) Backplane left 28 °C 60 °C 65 °C
3 OK Sensor (2) Backplane center 28 °C 60 °C 65 °C
4 OK Sensor (3) Backplane right 26 °C 60 °C 65 °C
5 OK Sensor (4) Processor SAS chip (TH1) 42 °C 70 °C 75 °C
6 OK Sensor (5) Processor board (TH2) 29 °C 70 °C 75 °C

Bild 78: Einzelheiten zu RAID-Festplatteneinheiten (Informationen zu ETERNUS JX40)

*Locate*

Aktiviert die Identifizierungs-LED der RAID-Festplatteneinheit.

## RAID-Festplatteneinheit: ETERNUS JX60

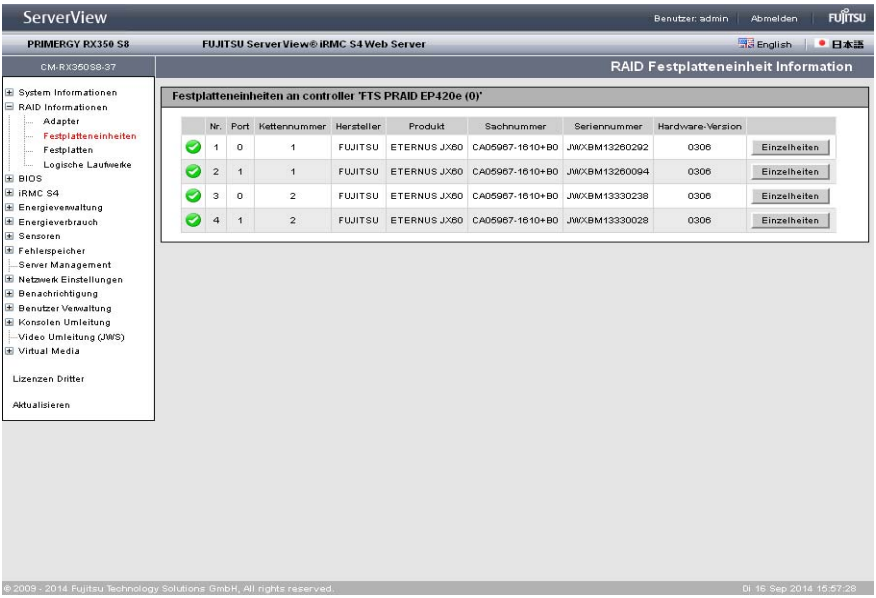



Bild 79: RAID-Informationen – Seite für RAID-Festplatteneinheiten (ETERNUS JX60)

*Einzelheiten*

Durch Klicken auf *Einzelheiten* wird eine neue Seite geöffnet, die detaillierte Informationen zur entsprechenden RAID-Festplatteneinheit enthält.

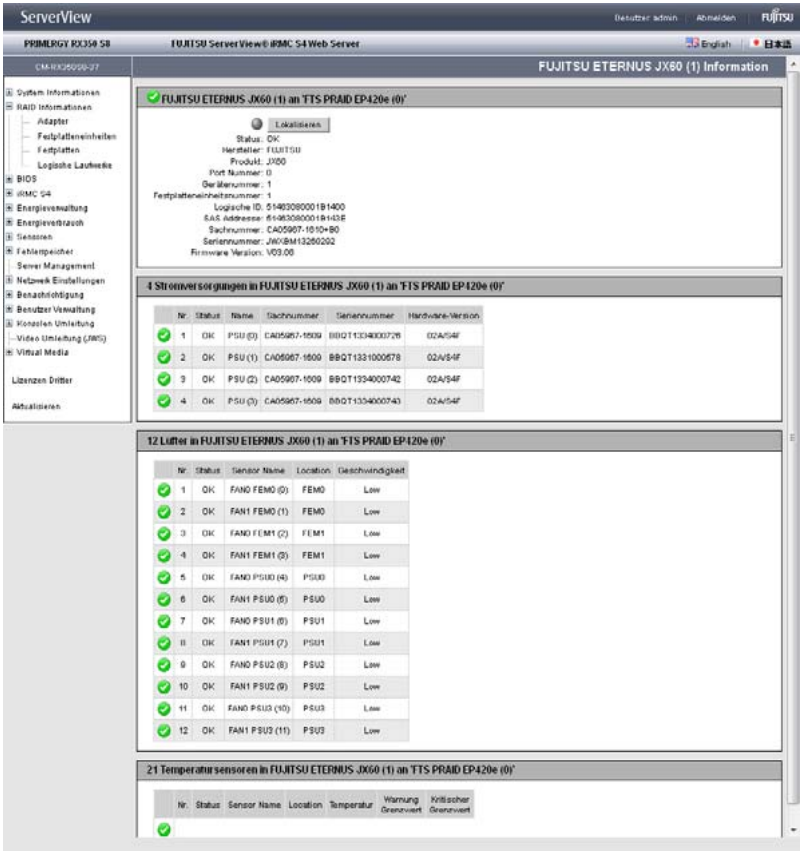

ServerView
PRIMERGY RX350 S8
FUJITSU ServerView® iRMC S4 Web Server
FUJITSU ETERNUS JX60 (1) Information
System Informationen
RAID Informationen
Adapter
Festplatteneinheiten
Festplatten
Logische Laufwerke
BIOS
iRMC S4
Energieverwaltung
Energieverbrauch
Sensoren
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigung
Benutzer Verwaltung
Konsolen Umleitung
Video Umleitung (JWS)
Virtual Media
Lizenzen Dritter
Aktualisieren
FUJITSU ETERNUS JX60 (1) an 'FTS PRAID EP420e (0)'
Lokalisieren
Status: OK
Hersteller: FUJITSU
Produkt: JX60
Port Nummer: 0
Geräteanzahl: 1
Festplatteneinheitsnummer: 1
Logische ID: 51463080001B1400
SAS Addresse: 51463080001B143E
Sachnummer: CA05907-1610+B0
Seriennummer: JW0BM13260202
Firmware Version: V03.06
4 Stromversorgungen in FUJITSU ETERNUS JX60 (1) an 'FTS PRAID EP420e (0)'
Nr. Status Name Sachnummer Seriennummer Hardware-Version
1 OK PSU (0) CA05907-1609 BBQT1334000726 02A/54F
2 OK PSU (1) CA05907-1609 BBQT1331000578 02A/54F
3 OK PSU (2) CA05907-1609 BBQT1334000742 02A/54F
4 OK PSU (3) CA05907-1609 BBQT1334000743 02A/54F
12 Lüfter in FUJITSU ETERNUS JX60 (1) an 'FTS PRAID EP420e (0)'
Nr. Status Sensor Name Location Geschwindigkeit
1 OK FAN0 FEM0 (0) FEM0 Low
2 OK FAN1 FEM0 (1) FEM0 Low
3 OK FAN0 FEM1 (2) FEM1 Low
4 OK FAN1 FEM1 (3) FEM1 Low
5 OK FAN0 PSU0 (4) PSU0 Low
6 OK FAN1 PSU0 (5) PSU0 Low
7 OK FAN0 PSU1 (6) PSU1 Low
8 OK FAN1 PSU1 (7) PSU1 Low
9 OK FAN0 PSU2 (8) PSU2 Low
10 OK FAN1 PSU2 (9) PSU2 Low
11 OK FAN0 PSU3 (10) PSU3 Low
12 OK FAN1 PSU3 (11) PSU3 Low
21 Temperatursensoren in FUJITSU ETERNUS JX60 (1) an 'FTS PRAID EP420e (0)'
Nr. Status Sensor Name Location Temperatur Warnung Grenzwert Kritischer Grenzwert

Bild 80: Einzelheiten zu RAID-Festplatteneinheiten (Informationen zu ETERNUS JX60)

*Locate*

Aktiviert die Identifizierungs-LED der RAID-Festplatteneinheit.

## 7.5.3 Festplatten - Informationen zu RAID Physikalische Laufwerke

Die Seite *Festplatten* enthält Informationen zu jedem RAID Physikalischen Laufwerk auf dem verwalteten Server.

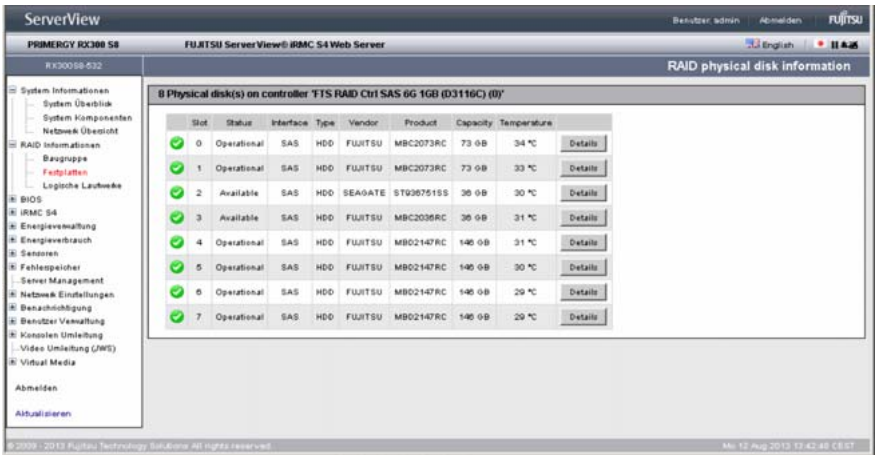

ServerView
Benutzer: admin
Abmelden
FUJITSU
PRIMERGY RX300 S8
FUJITSU ServerView® iRMC S4 Web Server
English
RX300S8-532
RAID physical disk information
System Informationen
System Überblick
System Komponenten
Netzwerk Übersicht
RAID Informationen
Baugruppe
Festplatten
Logische Laufwerke
BIOS
iRMC S4
Energieverwaltung
Energieverbrauch
Sensoren
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigung
Benutzer Verwaltung
Konsolen Umleitung
Video Umleitung (JWS)
Virtual Media
Abmelden
Aktualisieren
8 Physical disk(s) on controller 'FTS RAID Ctrl SAS 6G 1GB (D3116C) (0)'
Slot Status Interface Type Vendor Product Capacity Temperature
0 Operational SAS HDD FUJITSU MBC2073RC 73 GB 34 °C Details
1 Operational SAS HDD FUJITSU MBC2073RC 73 GB 33 °C Details
2 Available SAS HDD SEAGATE ST936751SS 36 GB 30 °C Details
3 Available SAS HDD FUJITSU MBC2036RC 36 GB 31 °C Details
4 Operational SAS HDD FUJITSU MBD2147RC 146 GB 31 °C Details
5 Operational SAS HDD FUJITSU MBD2147RC 146 GB 30 °C Details
6 Operational SAS HDD FUJITSU MBD2147RC 146 GB 29 °C Details
7 Operational SAS HDD FUJITSU MBD2147RC 146 GB 29 °C Details

Bild 81: RAID Informationen - Seite „Festplatten“

*Einzelheiten*

Durch Klicken auf *Details* wird eine neue Seite geöffnet, die detaillierte Informationen zum entsprechenden RAID Physikalischen Laufwerk enthält.

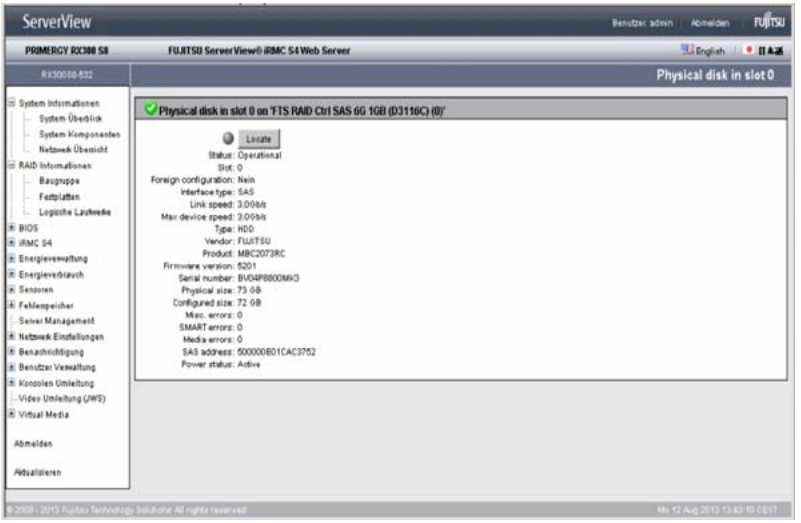



Bild 82: Details zu RAID Physikalischen Laufwerken

*Locate*

Aktiviert die Identifizierungs-LED des RAID Physikalischen Laufwerks.

## 7.5.4 Logische Laufwerke - Informationen über logische RAID-Laufwerke

Die Seite *Logische Laufwerke* enthält Informationen zu jedem logischen RAID-Laufwerk auf dem verwalteten Server.

Bild 83: RAID Informationen - Seite „Logische Laufwerke“

*Details*

Durch Klicken auf *Details* wird eine neue Seite geöffnet, die detaillierte Informationen zum entsprechenden logischen RAID-Laufwerk enthält.

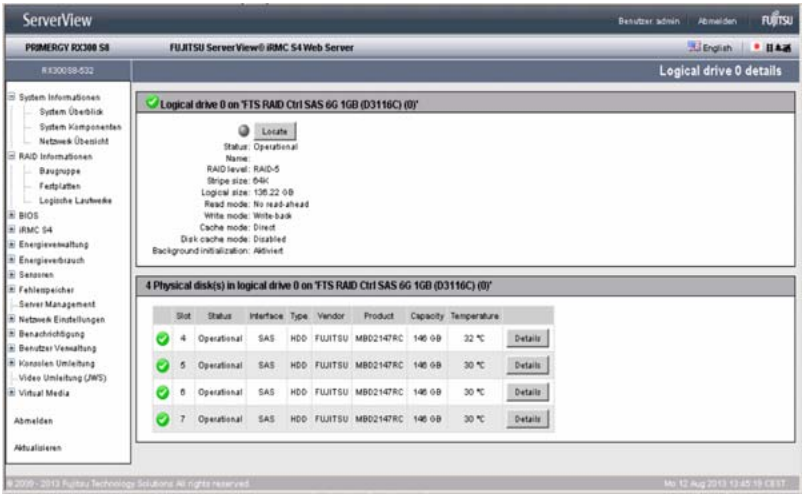



Bild 84: Details zu logischen Laufwerken

*Locate*

Aktiviert die Identifizierungs-LED des RAID Physikalischen Laufwerks, auf dem sich das logische Laufwerk befindet.

# 7.6 BIOS-Einstellungen sichern/wiederherstellen, BIOS aktualisieren

Der Eintrag *BIOS* enthält Links zu den folgenden Seiten:


– "BIOS-Parameter und -Einstellungen in Datei sichern / aus Datei wiederherstellen" auf Seite 180

– "BIOS aktualisieren via "Aktualisierung aus Datei" oder via TFTP" auf Seite 185


Diese Seiten werden nur dann angezeigt, wenn das BIOS des verwalteten Servers die entsprechenden funktionalen Anforderungen unterstützt.

## 7.6.1 BIOS-Parameter und -Einstellungen in Datei sichern / aus Datei wiederherstellen

Die Seite *BIOS Parameter und Einstellungen sichern/wiederherstellen* bietet Ihnen folgende Möglichkeiten:

– Einstellungen einzelner BIOS-Parameter im ServerView® WinSCU XML-Format sichern und die Sicherung in einer Datei speichern.

– Einstellungen einzelner BIOS-Parameter im ServerView® WinSCU XML-Format auf Basis einer Sicherungsdatei wiederherstellen.

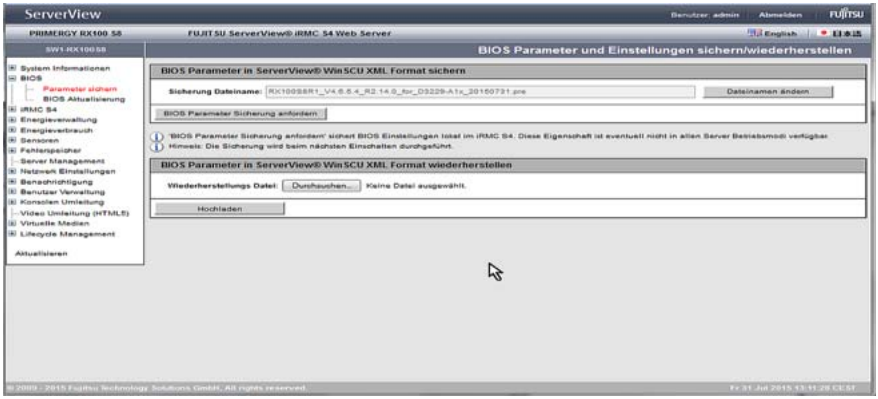


Bild 85: Seite BIOS Parameter und Einstellungen sichern/wiederherstellen

#### 7.6.1.1 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format sichern

Mit der Gruppe *BIOS Parameter in ServerView® WinSCU XML format sichern* können Sie die Einstellungen einzelner BIOS parameter im ServerView® WinSCU XML sichern und die Sicherung in einer Datei speichern.

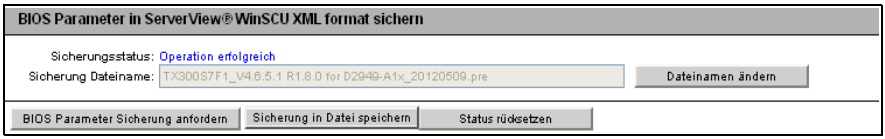

BIOS Parameter in ServerView® WinSCU XML format sichern
Sicherungsstatus: Operation erfolgreich
Sicherung Dateiname: TX300S7F1_V4.6.5.1 R1.8.0 for D2949-A1x_20120509.pre
Dateinamen ändern
BIOS Parameter Sicherung anfordern
Sicherung in Datei speichern
Status rücksetzen

Bild 86: BIOS-Parameter im ServerView® WinSCU XML-Format sichern

*Sicherungsstatus*

Wird nur dann angezeigt, wenn die Sicherung gerade durchgeführt wird oder abgeschlossen ist: Zeigt den Status des aktuellen Sicherungsprozesses an. Ein erfolgreicher Abschluss wird durch "Operation erfolgreich" angezeigt.

Zum Löschen der Anzeige klicken Sie auf die Schaltfläche *Status zurücksetzen*, die nur dann vorhanden ist, wenn zurzeit ein Status angezeigt wird.

*Status zurücksetzen*

Löscht die unter *Sicherungsstatus* angezeigte Statusinformation. Diese Schaltfläche ist nur dann vorhanden, wenn zurzeit unter *Sicherungsstatus* ein Status angezeigt wird.

*Sicherung Dateiname*

Dieses Eingabefeld ist standardmäßig deaktiviert ("ausgegraut"). Vorbelegt ist es mit dem vom iRMC dynamisch generierten Dateinamen.

*Dateinamen ändern*

Aktiviert das Feld *Sicherung Dateiname*, sodass Sie einen Dateinamen (*.pre*) Ihrer Wahl eingeben können.

*Dateiname speichern*

Sichert den geänderten Dateinamen, der ab sofort standardmäßig im Feld *Sicherung Dateiname* angezeigt wird.

*BIOS Parameter Sicherung anfordern*

Startet die Sicherung einzelner BIOS-Parameter-Einstellungen im ServerView® WinSCU XML format. Die Sicherung (mit dem im Feld *Sicherung Dateiname* angezeigten Namen) wird lokal am iRMC S4 gespeichert.

Sobald der Sicherungsprozess gestartet ist, wird der aktuelle Prozessstatus unter *Sicherungsstatus* angezeigt.

**Hinweise zum Sicherungsprozess:**

- Während des Sicherungsprozesses sind alle Schaltflächen und Eingabefelder deaktiviert.
- Falls der Server ausgeschaltet ist, wird er automatisch eingeschaltet.
- Falls der Server eingeschaltet ist, ist ein Reboot erforderlich. Andernfalls verbleibt der Server im Zustand "Boot steht noch aus".
- Nach Abschluss des Sicherungsprozesses wird der Server ausgeschaltet.

*Sicherung in Datei speichern*

Wird nur dann angezeigt, wenn eine Sicherung einzelner BIOS-Parameter im ServerView® WinSCU XML-Format im lokalen Speicher des iRMC vorhanden ist:

Öffnet einen Browser-Dialog, über den Sie die iRMC-lokale Kopie der BIOS-Sicherungsdaten in eine Datei (<*beliebiger-name*>.*pre*) sichern können.

*Status zurücksetzen*

Nur dann vorhanden, wenn aktuell unter *Sicherungsstatus* ein Status angezeigt wird: Löscht die unter *Sicherungsstatus* angezeigte Statusinformation.

### 7.6.1.2 Einzelne BIOS-Parameter im ServerView® WinSCU XML-Format wiederherstellen

Mit der Gruppe *BIOS Parameter in ServerView® WinSCU XML format wiederherstellen* können Sie die Einstellungen einzelner BIOS-Parameter im ServerView® WinSCU XML-Format auf Basis einer Sicherungsdatei wiederherstellen.

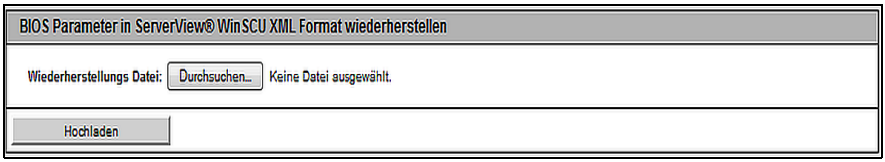



Bild 87: BIOS-Parameter im ServerView® WinSCU XML Format wiederherstellen

*Wiederherstellungsstatus*

Der *Wiederherstellungsstatus* wird nur dann angezeigt, wenn die Wiederherstellung gerade durchgeführt wird oder abgeschlossen ist: Zeigt den Status des aktuellen Wiederherstellungsprozesses an. Ein erfolgreicher Abschluss wird durch "Operation erfolgreich" angezeigt.

Zum Löschen der Anzeige klicken Sie auf die Schaltfläche *Status zurücksetzen*, die nur dann vorhanden ist, wenn zurzeit ein Status angezeigt wird.

*Wiederherstellungs Datei*

Ein Klick ins Eingabefeld oder auf *Durchsuchen...* öffnet einen Browser-Dialog, über den Sie zu einer Datei (*.pre*) navigieren können, die eine Sicherung einzelner BIOS-Parameter im ServerView® WinSCU XML-Format enthält.

*Upload*

Startet die Wiederherstellung einzelner BIOS-Parameter-Einstellungen auf Basis der im Feld *Wiederherstellungs Datei* spezifizierten Datei.

Sobald der Wiederherstellungsprozess gestartet ist, wird der aktuelle Prozessstatus unter *Wiederherstellungsstatus* angezeigt.

**Hinweise zum Wiederherstellungsprozess:**

- Während des Wiederherstellungsprozesses sind alle Schaltflächen und Eingabefelder deaktiviert.
- Falls der Server ausgeschaltet ist, wird er automatisch eingeschaltet.
- Falls der Server eingeschaltet ist, ist ein Reboot erforderlich. Andernfalls verbleibt der Server im Zustand "Boot steht noch aus".
- Nach Abschluss des Wiederherstellungsprozesses wird der Server ausgeschaltet.

*Status zurücksetzen*

Löscht die unter *Wiederherstellungsstatus* angezeigte Statusinformation. Diese Schaltfläche ist nur dann vorhanden, wenn zurzeit unter *Wiederherstellungsstatus* ein Status angezeigt wird.

## 7.6.2 BIOS aktualisieren via "Aktualisierung aus Datei" oder via TFTP

Die Seite *BIOS Einstellungen flashen* liefert Informationen zur aktuellen BIOS-Version auf dem verwalteten Server und ermöglicht es Ihnen, das BIOS via "Aktualisierung aus Datei" oder via TFTP zu aktualisieren.

Das zu Ihrem PRIMERGY Server passende BIOS-Image finden Sie auf der ServerView Suite DVD 2 bzw. zum Herunterladen unter *http://support.ts.fujitsu.com/com/support/downloads.html*.

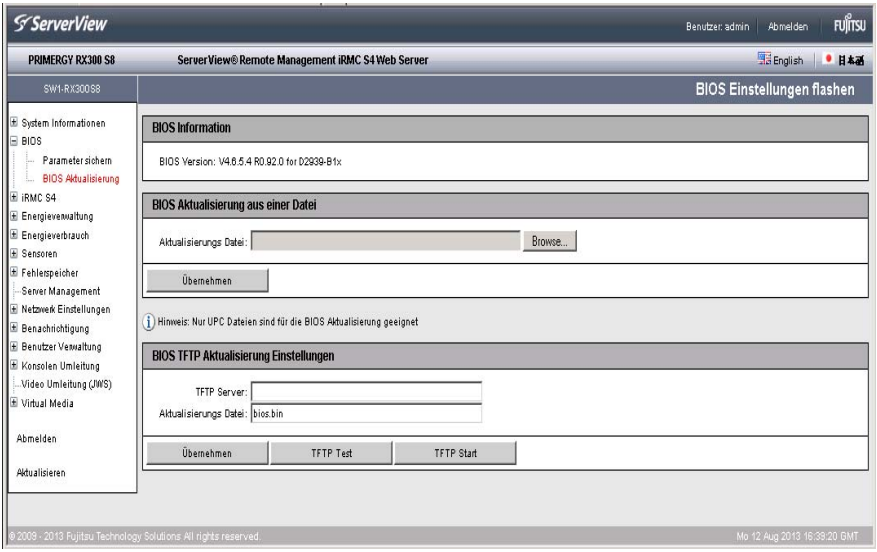


Bild 88: Seite BIOS Einstellungen flashen

### BIOS aktualisieren ("flashen") - Ablauf und wichtige Hinweise

Der folgende Überblick gilt sowohl für die BIOS-Aktualisierung via "Aktualisierung aus Datei" als auch für die BIOS-Aktualisierung via TFTP.

Einzelheiten zum Starten der in diesem Überblick beschriebenen Schritte sind weiter unten in diesem Abschnitt beschrieben.

Während des kompletten Aktualisierungsprozesses wird der aktuelle Status in der Seite *BIOS Einstellungen flashen* angezeigt.

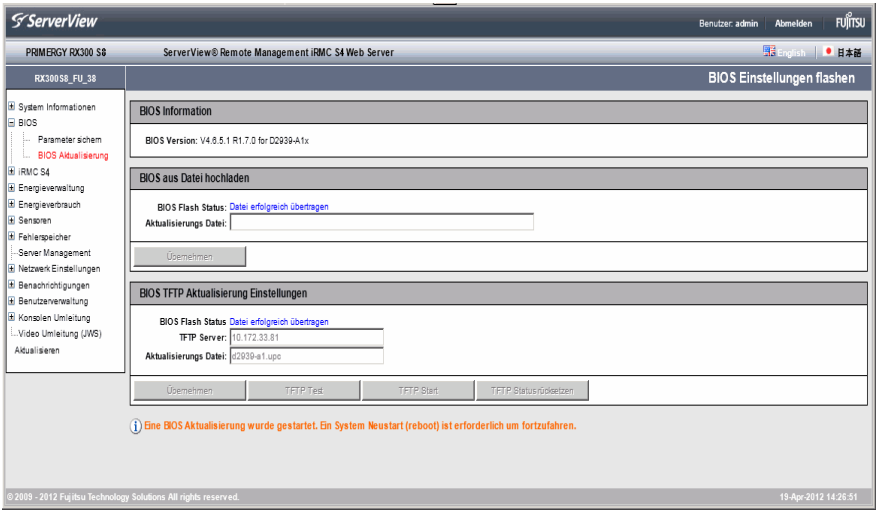



Bild 89: BIOS-Aktualisierung - (TFTP) Download erfolgreich abgeschlossen

Die BIOS-Aktualisierung umfass die folgenden Schritte:

1. Im ersten Schritt laden Sie die Aktualisierungsdatei herunter.

   Nach dem Herunterladen der Aktualisierungsdatei geht es wie folgt weiter:

   – Falls der Server ausgeschaltet ist, wird er für den Aktualisierungsprozess automatisch eingeschaltet.

   – Falls der Server bereits eingeschaltet ist, müssen Sie den Server für den Aktualisierungsprozess neu starten.

   **ACHTUNG!**

   Falls gerade eine BIOS-Aktualisierung durchgeführt wird: Schalten Sie den Server **nicht** aus und führen Sie auch keinen Neustart durch.

2. Anschließend werden die Aktualisierungsdaten (Flash-Daten) in den Speicher übertragen. Die Statusanzeige informiert, wenn die Übertragung erfolgreich abgeschlossen ist.

3. Vor dem Start des eigentlichen Flash-Prozesses wird das Flash/Aktualiserungs-Image geprüft.

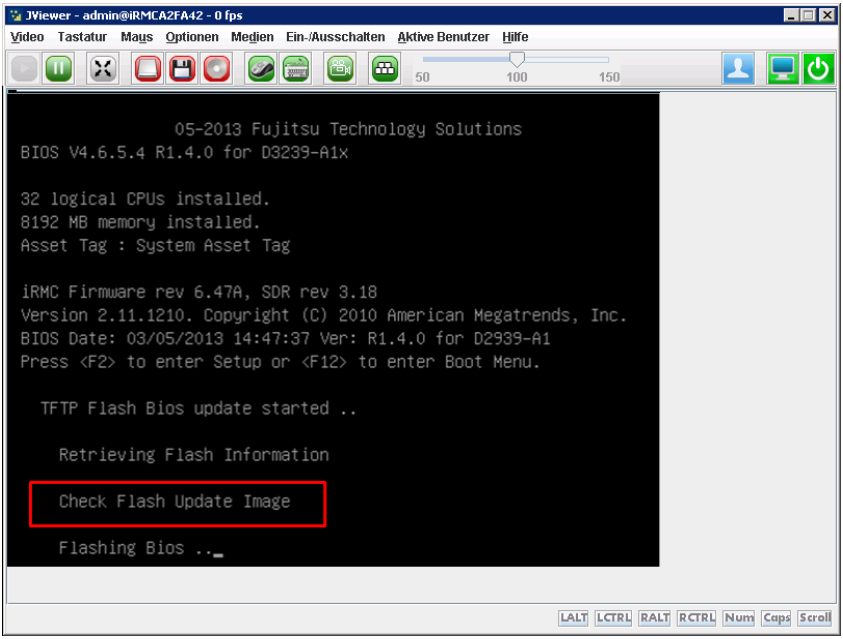

JViewer - admin@iRMCA2FA42 - 0 fps
Video Tastatur Maus Optionen Medien Ein-/Ausschalten Aktive Benutzer Hilfe
50 100 150
05-2013 Fujitsu Technology Solutions
BIOS V4.6.5.4 R1.4.0 for D3239-A1x
32 logical CPUs installed.
8192 MB memory installed.
Asset Tag : System Asset Tag
iRMC Firmware rev 6.47A, SDR rev 3.18
Version 2.11.1210. Copyright (C) 2010 American Megatrends, Inc.
BIOS Date: 03/05/2013 14:47:37 Ver: R1.4.0 for D2939-A1
Press <F2> to enter Setup or <F12> to enter Boot Menu.
TFTP Flash Bios update started ..
Retrieving Flash Information
Check Flash Update Image
Flashing Bios ..
LALT LCTRL RALT RCTRL Num Caps Scroll

Bild 90: BIOS aktualisieren - Update (Flash-Image) prüfen

4. Nach erfolgreicher Verifizierung des Flash/Aktualisierungs-Image wird der eigentliche Flash-Prozess gestartet. Die Statusanzeige informiert über den prozentualen Fortschritt des Flash-Prozesses.
5. Nach erfolgreichem Abschluss der BIOS-Aktualisierung schaltet sich der Server aus. Der folgende Eintrag wird in den Ereignisspeicher (System Event Log, SEL) geschrieben:

   `BIOS TFTP or HTTP/HTTPS flash OK`

### BIOS Information

Diese Gruppe informiert über die aktuelle BIOS-Version auf dem verwalteten Server.

### BIOS-Aktualisierung aus einer Datei

Mit der Gruppe *BIOS aus Datei hochladen* können Sie eine Online-Aktualisierung des BIOS auf dem verwalteten Server durchführen. Hierfür müssen Sie das aktuelle BIOS-Image in einer Datei bereitstellen.

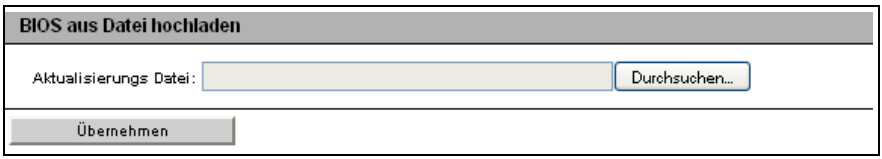



Bild 91: Seite BIOS Einstellungen flashen - BIOS aus Datei hochladen

*Aktualisierungs Datei*
Datei, in der das BIOS-Image gespeichert ist.

*Durchsuchen...*
Öffnet den Datei-Browser, über den Sie zur Aktualisierungsdatei navigieren können.

*Übernehmen*
Aktiviert Ihre Einstellungen und startet die BIOS-Aktualisierung.

**ACHTUNG!**

Falls gerade eine BIOS-Aktualisierung durchgeführt wird: Schalten Sie den Server **nicht** aus und führen Sie auch keinen Neustart durch.

### BIOS-Aktualisierung via TFTP

Mit der Gruppe *BIOS TFTP Aktualisierung Einstellungen* können Sie eine Online-Aktualisierung des BIOS auf dem verwalteten Server durchführen. Hierfür müssen Sie das aktuelle BIOS-Image in einer Datei auf einem TFTP-Server bereitstellen. Das BIOS wird aktualisiert, sobald TFTP gestartet ist.

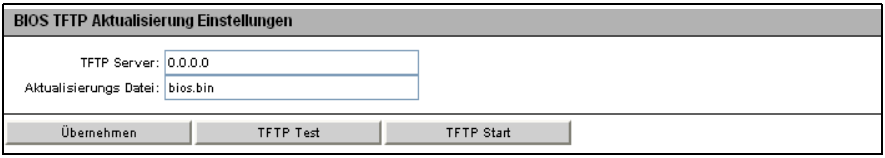



Bild 92: BIOS Update Settings page - BIOS TFTP Update Settings

*TFTP Server*
: IP-Adresse oder DNS-Name des TFTP-Servers, auf dem die Datei mit dem BIOS-Image gespeichert ist.

*Aktualisierungs Datei*
: Datei, in der das BIOS-Image gespeichert ist.

*Übernehmen*
: Aktiviert Ihre Einstellungen.

*TFTP Test*
: Testet die Verbindung zum TFTP-Server.

*TFTP Start*
: Lädt die Datei mit dem BIOS-Image vom TFTP-Server herunter und startet die BIOS-Aktualisierung.

**ACHTUNG!**

Falls gerade eine BIOS-Aktualisierung durchgeführt wird: Schalten Sie den Server **nicht** aus und führen Sie auch keinen Neustart durch.

# 7.7 iRMC S4 - Informationen, Firmware und Zertifikate

Der Eintrag *iRMC S4* enthält die Verweise auf folgende Seiten:


– "iRMC S4 Informationen – Informationen zum iRMC S4" auf Seite 191

– "iRMC S4 Zeit - Zeitoptionen für den iRMC S4" auf Seite 195

– "iRMC S4 Firmware Einstellungen abspeichern - Firmware-Einstellungen abspeichern" auf Seite 198

– "Zertifikat Austausch - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden" auf Seite 200.

– "Selbstsigniertes Zertifikat erzeugen - Selbstsigniertes RSA Zertifikat erzeugen" auf Seite 207

– "iRMC S4 Firmware Aktualisierung" auf Seite 209

### 7.7.1 iRMC S4 Informationen – Informationen zum iRMC S4

Die Seite *iRMC S4 Informationen* bietet Ihnen folgende Möglichkeiten:

– Informationen zu Firmware- und SDRR-Version des iRMC S4einsehen, den Firmware-Selektor setzen und den iRMC S4 neu starten.

– Informationen über aktive iRMC S4-Sitzungen einsehen.

– Lizenzschlüssel (License Key) auf den iRMC S4 laden.

– Einstellungen für das Layout der iRMC-Weboberfläche festlegen.

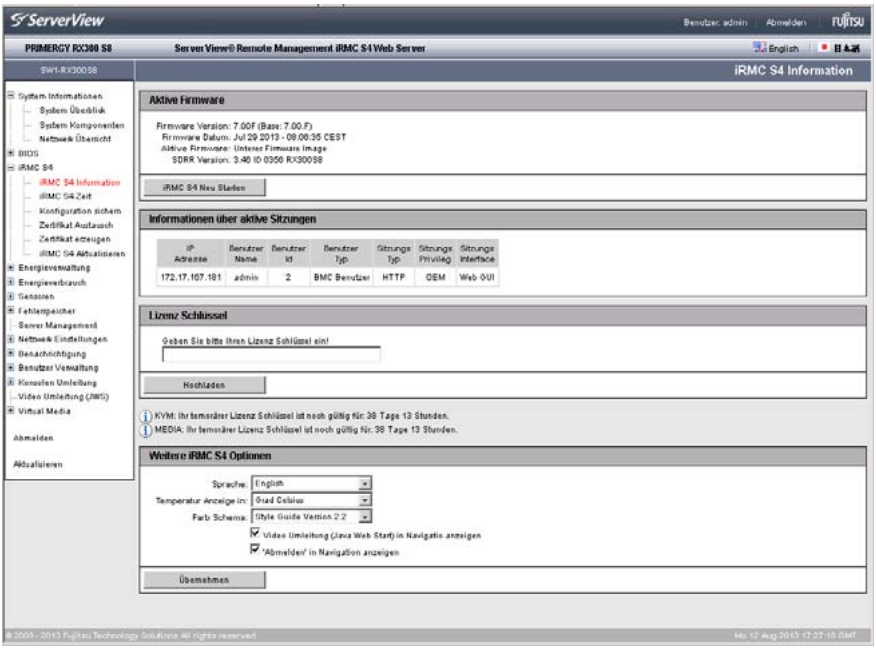


Bild 93: Seite iRMC S4 Information

### Aktive Firmware

Unter *Aktive Firmware* können Sie sich über Firmware- und SDRR-Version des iRMC S4 informieren und den iRMC S4 neu starten.

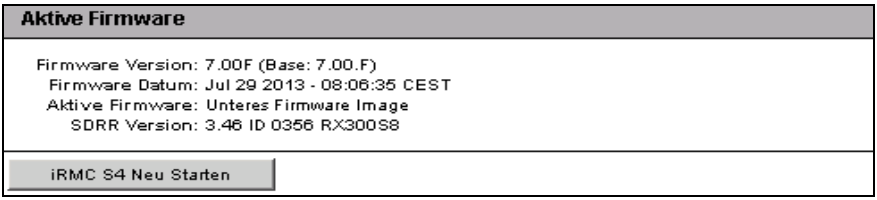

Aktive Firmware
Firmware Version: 7.00F (Base: 7.00.F)
Firmware Datum: Jul 29 2013 - 08:06:35 CEST
Aktive Firmware: Unteres Firmware Image
SDRR Version: 3.46 ID 0356 RX300S8
iRMC S4 Neu Starten

Bild 94: Seite iRMC S4 Informationen - Firmware Informationen und iRMC S4 neu starten

*iRMC S4. neu starten*

Startet den iRMC S4 neu..

Die Schaltfläche *iRMCS4 neu starten* ist während der BIOS POST-Phase des verwalteten Servers deaktiviert.

### Informationen über aktive Sitzungen

In der Gruppe *Informationen über aktive Sitzungen* werden alle zurzeit aktiven iRMC S4-Sitzungen angezeigt.

**Informationen über aktive Sitzungen**

| IP Adresse | Benutzer Name | Benutzer Id | Sitzungs Typ | Sitzungs Privileg | Sitzungs Interface | Port der Gegenstelle |
|---|---|---|---|---|---|---|
| 217.9.101.18 | admin | 2 | HTTP | OEM | Web GUI | 1194 |
| 172.25.88.120 | admin | 2 | IPMI 1.5 | Administrator | IPMI | 1181 |

Bild 95: Seite iRMC S4 Informationen Informationen über aktive Sitzungen

### Lizenz Schlüssel (License Key)

Mit der Gruppe *Lizenz Schlüssel* können Sie einen Lizenzschlüssel auf den iRMC S4 laden.

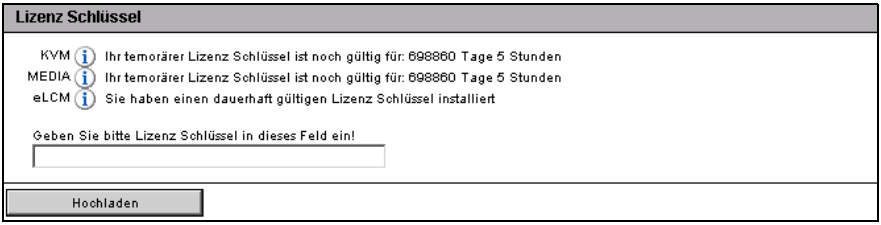

Lizenz Schlüssel
KVM Ihr temorärer Lizenz Schlüssel ist noch gültig für: 698860 Tage 5 Stunden
MEDIA Ihr temorärer Lizenz Schlüssel ist noch gültig für: 698860 Tage 5 Stunden
eLCM Sie haben einen dauerhaft gültigen Lizenz Schlüssel installiert
Geben Sie bitte Lizenz Schlüssel in dieses Feld ein!
Hochladen

Bild 96: Seite iRMC S4 Informationen Lizenz Schlüssel

Sie benötigen einen gültigen Lizenzschlüssel, um die iRMC S4-Funktionen *Advanced Video Redirection* (siehe Seite 346), *Virtual Media* (siehe Seite 356) und *Lifecycle Management* (siehe Seite 363) nutzen zu können. Der Lizenzschlüssel für die Lebenszyklusverwaltung wird immer zusammen mit der SD-Karte des iRMC S4 gekauft.

Den Lizenzschlüssel können Sie käuflich erwerben. Der Lizenzschlüssel für die Lebenszyklusverwaltung wird immer zusammen mit der SD-Karte des iRMC S4 gekauft.

*Hochladen*

Wenn Sie auf diese Schaltfläche klicken, wird der im Eingabefeld spezifizierte Lizenzschlüssel auf den iRMC S4 geladen.

### Weitere iRMC S4 Optionen

Mit der Gruppe *Weitere iRMC S4 Optionen* können Sie Einstellungen für das Layout der iRMC-Weboberfläche festlegen.

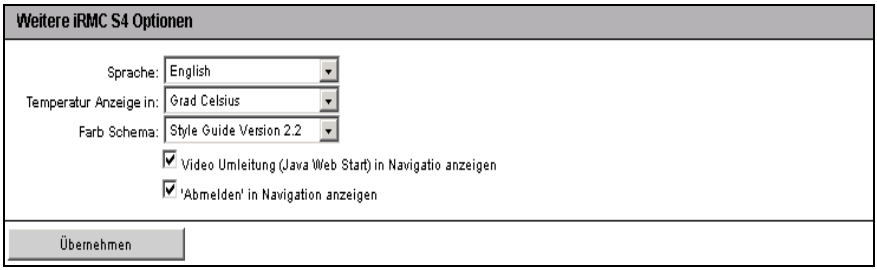

Weitere iRMC S4 Optionen
Sprache: English
Temperatur Anzeige in: Grad Celsius
Farb Schema: Style Guide Version 2.2
Video Umleitung (Java Web Start) in Navigatio anzeigen
'Abmelden' in Navigation anzeigen
Übernehmen

Bild 97: iRMC S2/S3 Information - Weitere iRMC S2/S3 Optionen

*Sprache*

Legt die Landessprache (Deutsch/Englisch/Japanisch) fest, die beim nächsten Aufruf der iRMC S4-Weboberfläche voreingestellt ist.

*Temperatur Anzeige in*

Legt die Einheit für die Anzeige von Temperaturwerten an der iRMC S4-Weboberfläche fest (Grad Celsius / Grad Fahrenheit). Diese Einstellung gilt für die aktuelle Sitzung und ist beim nächsten Aufruf der iRMC S4-Weboberfläche voreingestellt.

*Farb Schema*

Legt das Farbschema für die Anzeige der iRMC S4-Weboberfläche fest. Diese Einstellung gilt für die aktuelle Sitzung und ist beim nächsten Aufruf der iRMC S4-Weboberfläche voreingestellt.

*Video Umleitung(Java Web Start) in Navigation anzeigen*

Fügt dem Navigationsbereich den Link *Video Umleitung (JWS)* hinzu. Dadurch können Sie die Video-Umleitung (Java Web Start) direkt starten (siehe "Video Umleitung - AVR mit Java starten" auf Seite 353).

*'Abmelden' in Navigation anzeigen*

Diese Option wird nur angeboten, wenn die Seite iRMC S4 im Farbschema *StyleguideVersion 2.2* angezeigt wird.

Fügt dem Navigationsbereich den Link *Abmelden* hinzu. Auf diese Weise können Sie sich vom Navigationsbereich aus abmelden.

*"Automatisch übernehmen" aktivieren*

Alle Einstellungen werden aktiviert, sobald sie festgelegt werden. Die Schaltflächen *Übernehmen* auf den einzelnen Seiten des iRMC S4 sind ausgeblendet, bis die Auswahl der Option *"Automatisch übernehmen" aktivieren* wieder aufgehoben wurde.

*Übernehmen*

Wendet die ausgewählte Option an.

## 7.7.2 iRMC S4 Zeit - Zeitoptionen für den iRMC S4

Mithilfe der Seite *iRMC S4 Zeit* konfigurieren Sie die Zeiteinstellungen des iRMC.

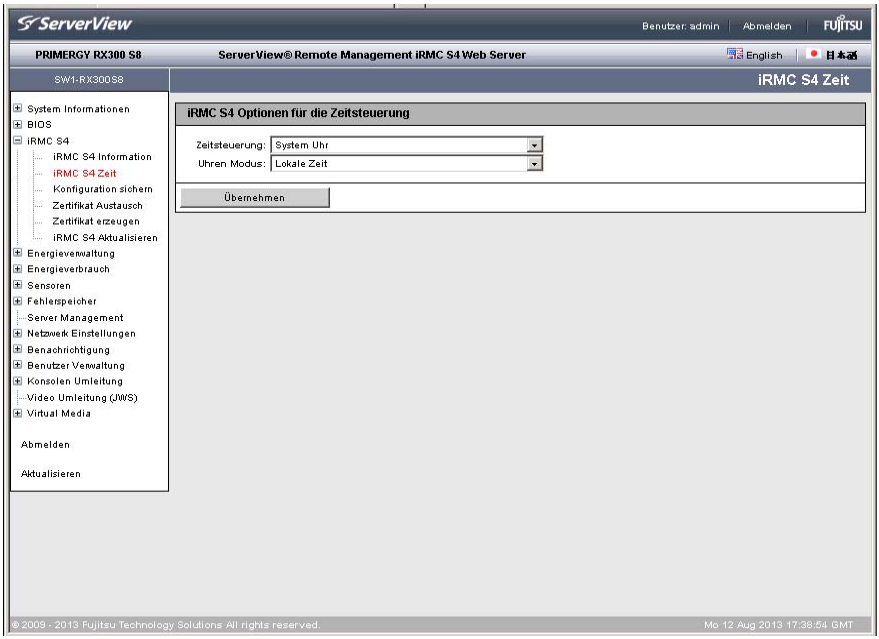



Bild 98: Seite iRMC S4 Zeit

### iRMC S4-Zeiteinstellungen

Mithilfe der Gruppe *iRMC S4 Optionen für die Zeitsteuerung* konfigurieren Sie die Zeiteinstellungen des iRMC S4.

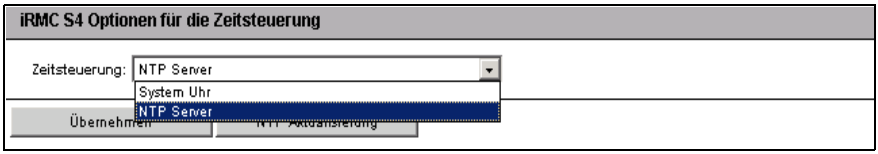



Bild 99: Seite iRMC S4 Zeit - iRMC S4 Optionen für die Zeitsteuerung

*Zeitsteuerung*

Hier können Sie auswählen, ob der iRMC S4 die Zeiteinstellungen vom verwalteten Server oder einem NTP-Server erhält.

*System Uhr*

Der iRMC S4 übernimmt die Zeit der Systemuhr des verwalteten Servers.

*NTP Server*

Der iRMC S4 verwendet das Network Time Protocol (NTP), um die eigene Uhrzeit mit der eines NTP-Servers zu synchronisieren, der als Referenzquelle für die Zeit dient.

Wenn Sie diese Option aktivieren, wird eine zusätzliche Gruppe angezeigt, die Gruppe *NTP (Network Time Protocol) Konfiguration*, mit der Sie die erforderlichen NTP-Einstellungen konfigurieren können (siehe unten).

*Uhren Modus*

Hier können Sie auswählen, ob die iRMC S4-Uhrzeit ab sofort im UTC-Format (Universal Time Coordinated) oder im Format „Lokale Zeit“ angezeigt wird.

*UTC (Universal Time Coordinated)*

Die iRMC S4-Uhrzeit wird im UTC-Format (Universal Time Coordinated) angezeigt.

*Lokale Zeit*

Die iRMC S4-Uhrzeit wird im Format „Lokale Zeit“ angezeigt.

### Konfiguration der Zeitzone

In dieser Gruppe können Sie die Zeitzone entsprechend dem Standort des PRIMERGY Servers konfigurieren.

*Zeitzone*
Liste der Zeitzonen.

*Übernehmen*
Wendet die ausgewählten Einstellungen an.

### NTP (Network Time Protocol) Konfiguration

Die Gruppe *NTP (Network Time Protocol) Konfiguration* ermöglicht es Ihnen, die erforderlichen NTP-Einstellungen zu konfigurieren, wenn die Option *NTP Server* in der Gruppe *iRMC S4 Optionen für die Zeitsteuerung* aktiviert wurde.

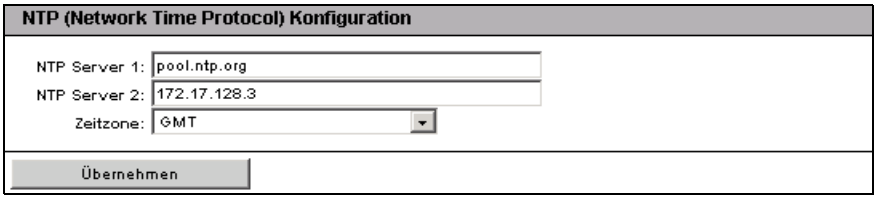



Bild 100: Seite iRMC S4 Zeit - NTP-Konfiguration

*NTP Server 1*
IP-Adresse oder DNS-Name des primären NTP-Servers.

*NTP Server 2*
IP-Adresse oder DNS-Name des sekundären NTP-Servers.

*Zeitzone*
Konfigurieren Sie die *Zeitzone* entsprechend dem Standort des PRIMERGY-Servers.

*Übernehmen*
Aktiviert die Einstellungen dieser Gruppe.

## 7.7.3 iRMC S4 Firmware Einstellungen abspeichern - Firmware-Einstellungen abspeichern

Mithilfe der Seite *iRMC S4 Firmware Einstellungen abspeichern* können Sie die aktuellen Firmware-Einstellungen sowie eine Reihe weiterer Einstellungen des iRMC in einer Datei abspeichern. Zusätzlich können Sie die Firmware-Einstellungen erneut auf den iRMC laden.

Wenn Sie die Benutzereinstellungen *(Benutzer Einstellungen)* speichern möchten, benötigen Sie die Berechtigung *Configure User Accounts*. Für alle anderen Fälle ist die Berechtigung *Configure iRMC S4 Settings* ausreichend.

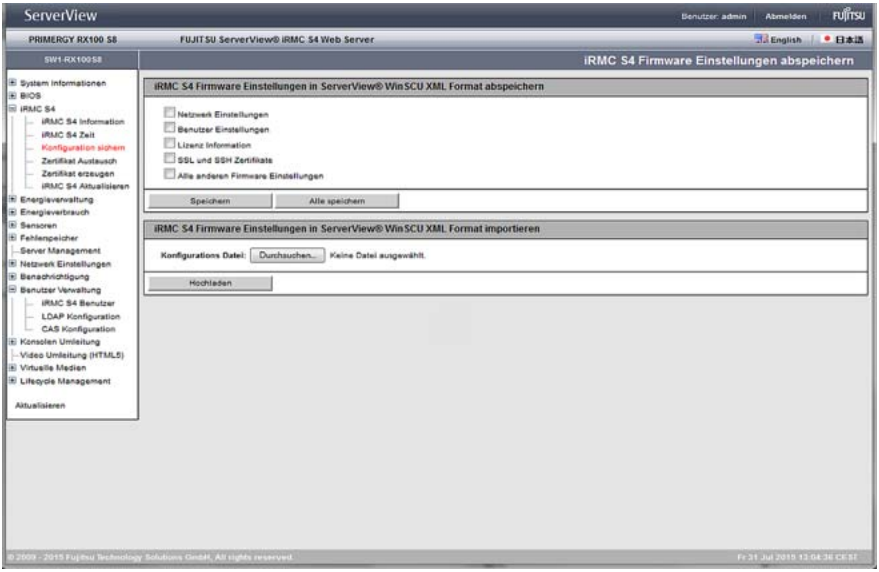



Bild 101: Seite „iRMC S4 Firmware Einstellungen abspeichern“

### iRMC S4 Firmware Einstellungen abspeichern...

Die Daten werden aus dem iRMC in logische Abschnitte exportiert, die jeweils einer ausgewählten Option entsprechen.

Die Option *Alle anderen Firmware Einstellungen* sorgt dafür, dass die Firmware alle aktuellen ConfigSpace-Werte exportiert, die noch nicht zusammen mit einem anderen Abschnitt exportiert wurden. Neu implementierte Werte werden automatisch mit neueren Firmware-Versionen exportiert.

*Speichern*
Mit *Speichern* sichern Sie die gewählten Einstellungen.

*Alle speichern*
Mit *Alle speichern* sichern Sie alle Einstellungen.

### iRMC S4 Firmware Einstellungen in ServerView® WinSCU XML Format importieren

*Konfigurations Datei*
Konfigurationsdatei (Standard: *iRMC_S4_settings.bin*) im ServerView® WinSCU XML-Format, aus der Sie die Firmware-Einstellungen auf den iRMC laden möchten.

*Durchsuchen...*
Öffnet einen Datei-Browser, mit dem Sie zu der Konfigurationsdatei navigieren können.

*Hochladen*
Lädt die Firmware-Einstellung in ausgewählte Datei hoch.

### 7.7.4 Zertifikat Austausch - DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel laden

Mit der Seite *Zertifikat Austausch* können Sie ein von einer Zertifizierungsstelle (Certificate Authority, CA) signiertes X.509 DSA/RSA-Zertifikat und/oder Ihren privaten DSA/RSA-Schlüssel auf den iRMC laden.

Der iRMC wird mit einem vordefinierten Server-Zertifikat (Standard-Zertifikat) ausgeliefert. Wenn Sie über SSL/TSL-gesicherte Verbindungen auf den iRMC zugreifen möchten, wird empfohlen, das Standard-Zertifikat möglichst bald durch ein Zertifikat zu ersetzen, das von einer Zertifizierungsstelle signiert ist.

Eingabeformat von X.509 DSA/RSA-Zertifikat und privatem DSA/RSA-Schlüssel:

X.509 DSA/RSA-Zertifikat und privater RSA/DSA-Schlüssel müssen jeweils in PEM-Codierung (ASCII/Base64) vorliegen.

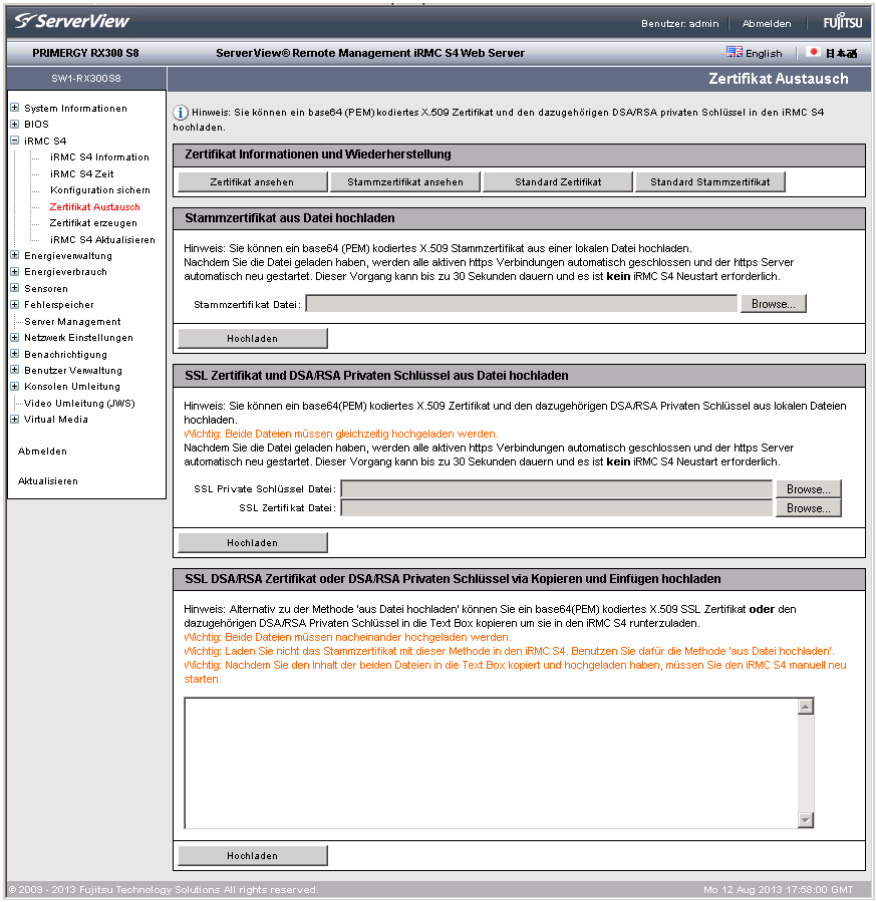


Bild 102: Seite Zertifikat Austausch

### Aktuell gültiges DSA/RSA-Zertifikat / Stammzertifikat anzeigen

- Klicken Sie in der Gruppe *Zertifikat Informationen und Wiederherstellung* auf die Schaltfläche *Zertifikat ansehen*, um sich das aktuell gültige Zertifikat anzeigen zu lassen.
- Klicken Sie in der Gruppe *Zertifikat Informationen und Wiederherstellung* auf die Schaltfläche *Stammzertifikat ansehen*, um sich das aktuell gültige Stammzertifikat (CA Certifikate) anzeigen zu lassen.

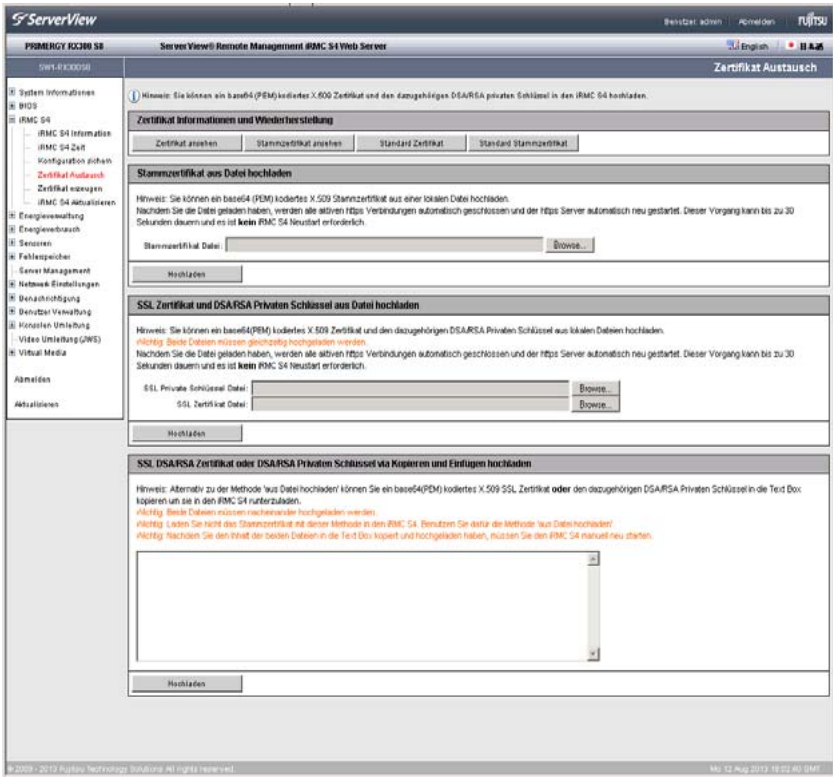



Bild 103: Seite Zertifikat Austausch - Anzeige des aktuell gültigen SSH/SSL-Zertifikats

### Standard-Zertifikat /Stammzertifikat wiedereinsetzen

- Klicken Sie in der Gruppe *Zertifikat Informationen und Wiederherstellung* auf die Schaltfläche *Standard Zertifikat*, um nach einem Bestätigungsdialog das Standard-Zertifikat wiedereinzusetzen, das mit der Firmware ausgeliefert wurde.
- Klicken Sie in der Gruppe *Zertifikat Informationen und Wiederherstellung* auf die Schaltfläche *Standard Stammzertifikat*, um nach einem Bestätigungsdialog das Standard-Stammzertifikat wiedereinzusetzen, das mit der Firmware ausgeliefert wurde.

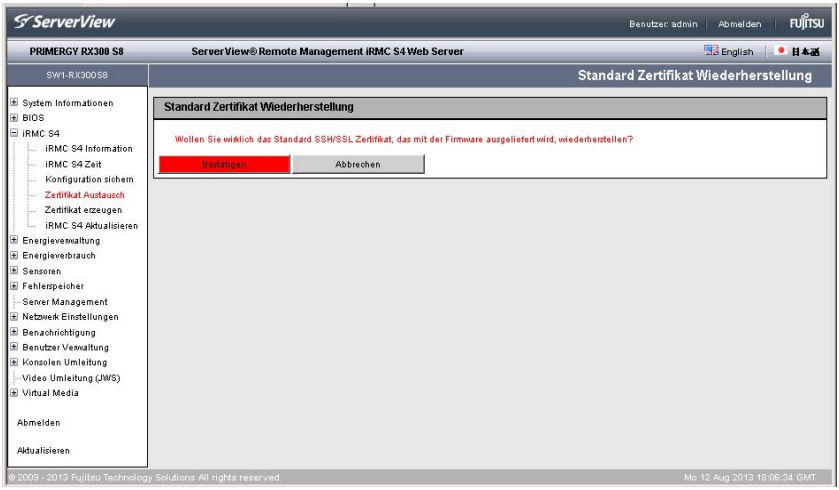


Bild 104: Seite Zertifikat Austausch - Standard Stammzertifikat wiedereinsetzen

### Stammzertifikat aus einer lokalen Datei hochladen

Um ein Stammzertifikat aus einer lokalen Datei auf den iRMC S2/S3 zu laden, verwenden Sie die Gruppe *Stammzertifikat aus Datei hochladen*.

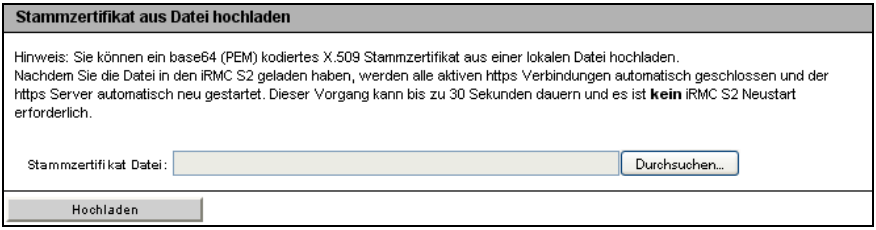



Bild 105: Stammzertifikat aus einer lokalen Datei hochladen

Gehen Sie wie folgt vor:

- ► Speichern Sie das Stammzertifikat in einer lokalen Datei an Ihrem Remote-Arbeitsplatz.
- ► Spezifizieren Sie die Datei unter *Stammzertifikat Datei*, indem Sie auf die zugehörige Schaltfläche *Durchsuchen...* klicken und zur Datei navigieren, die das Stammzertifikat enthält.
- ► Klicken Sie auf die Schaltfläche *Hochladen*, um das Stammzertifikat auf den iRMC zu laden.

  Beim Hochladen des Stammzertifikats werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Dieser Vorgang kann bis zu 30 Sekunden dauern.

  Ein expliziter Neustart des iRMC ist **nicht** erforderlich.

- ► Klicken Sie auf die Schaltfläche *Stammzertifikat ansehen*, um sich vom erfolgreichen Hochladen des Stammzertifikats zu überzeugen.

### DSA/RSA-Zertifikat / privaten DSA/RSA-Schlüssel direkt eingeben

Hierfür verwenden Sie die Gruppe
*SSL Zertifikat und DSA/RSA Privaten Schlüssel aus Datei hochladen*.

Privater Schlüssel und Zertifikat müssen gleichzeitig auf den iRMC S4 geladen werden.

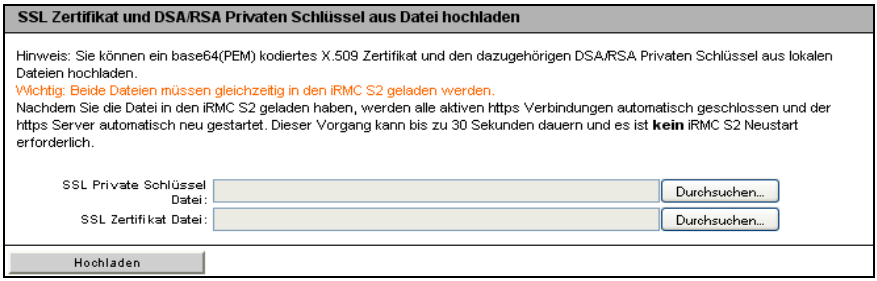



Bild 106: DSA/RSA-Zertifikat und privaten DSA/RSA-Schlüssel aus lokalen Dateien hochladen

Gehen Sie wie folgt vor:

- Speichern Sie das X.509 DSA/RSA-Zertifikat und den privaten DSA/RSA-Schlüssel jeweils in einer lokalen Datei an Ihrem Remote-Arbeitsplatz.
- Spezifizieren Sie unter *SSL Private Schlüssel Datei* und *SSL Zertifikat Datei* die Dateien für den privaten Schlüssel und das Zertifikat, indem Sie jeweils auf die zugehörige Schaltfläche*Durchsuchen...* klicken und zur Datei navigieren, die den privaten Schlüssel bzw. das Zertifikat enthält.
- Klicken Sie auf *Hochladen*, um das Zertifikat und den privaten Schlüssel auf den iRMC zu laden.

  Beim Hochladen von Zertifikat und privatem Schlüssel werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Dieser Vorgang kann bis zu 30 Sekunden dauern.

  Ein expliziter Neustart des iRMC ist **nicht** erforderlich.
- Klicken Sie auf die Schaltfläche *Zertifikat ansehen*, um sich vom erfolgreichen Hochladen des Zertifikats zu überzeugen.

### DSA/RSA-Zertifikat / privaten DSA/RSA-Schlüssel direkt eingeben

Hierfür verwenden Sie die Gruppe *SSL DSA/RSA Zertifikat oder DSA/RSA Privaten Schlüssel via Kopieren und Einfügen hochladen*.

Verwenden Sie dieses Verfahren **nicht**, um ein Stammzertifikat auf den iRMC zu laden. Laden Sie ein Stammzertifikat immer via Datei (siehe Seite 205).

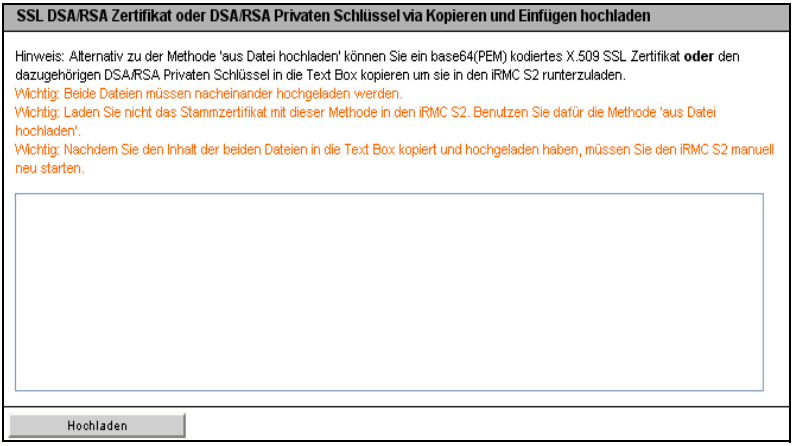



Bild 107: DSA/RSA-Zertifikat / privaten DSA/RSA-Schlüssel direkt eingeben

Gehen Sie wie folgt vor:

- Kopieren Sie das X.509 DSA-Zertifikat **oder** den privaten DSA-Schlüssel in den Eingabebereich.

  Die gleichzeitige Eingabe von Zertifikat und Schlüssel für denselben Ladevorgang ist nicht zulässig.

- Klicken Sie auf *Hochladen*, um das Zertifikat oder den privaten Schlüssel auf den iRMC zu laden.

- Führen Sie mithilfe des Remote Manager einen Neustart (Reset) des iRMC S4 durch (siehe Abschnitt "Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S4" auf Seite 404).

  Dies ist erforderlich, damit ein auf den iRMC geladenes Zertifikat oder privater Schlüssel gültig wird.

- Klicken Sie auf die Schaltfläche *Zertifikat ansehen*, um sich vom erfolgreichen Hochladen des Zertifikats zu überzeugen.

## 7.7.5 Selbstsigniertes Zertifikat erzeugen - Selbstsigniertes RSA Zertifikat erzeugen

Mit der Seite *Selbstsigniertes RSA Zertifikat erzeugen* können Sie ein selbstsigniertes RSA-Zertifikat erstellen.

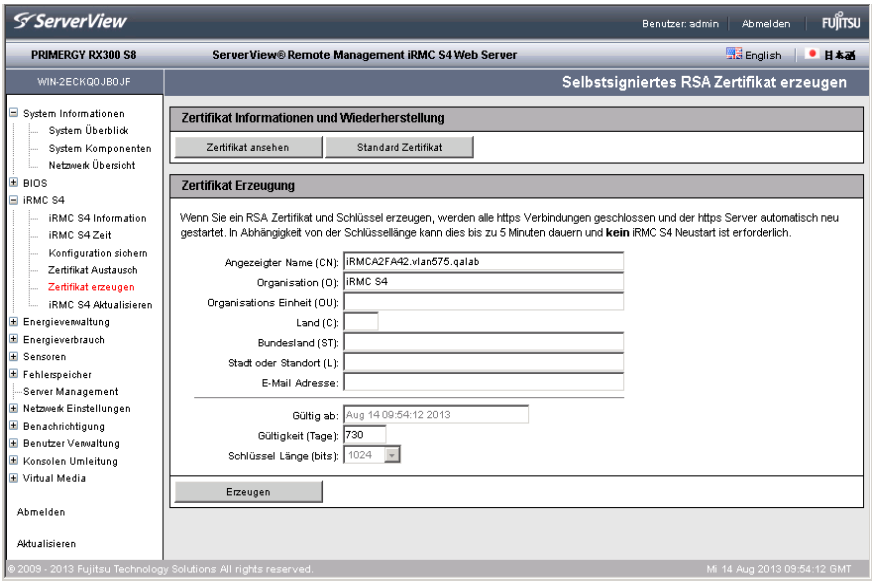


Bild 108: Seite Selbstsigniertes RSA Zertifikat erzeugen

### Zertifikat Informationen und Wiederherstellung

Mit der Gruppe *Zertifikat Informationen und Wiederherstellung* können Sie sich das aktuell gültige DSA/RSA-Zertifikat ansehen und/oder das Standard-RSA/DSA-Zertifikat wiedereinsetzen.

*Zertifikat ansehen*
: Mithilfe dieser Schaltfläche können Sie sich das aktuell gültige DSA/RSA-Zertifikat anzeigen lassen.

*Standard Zertifikat*
: Mithilfe dieser Schaltfläche können Sie über einen Bestätigungsdialog das Standard-Zertifikat wiedereinsetzen, das mit der Firmware ausgeliefert wurde.

### Zertifikat Erzeugung

Um ein selbstsigniertes RSA-Zertifikat zu erzeugen, gehen Sie wie folgt vor:

- Tragen Sie unter *Zertifikat Erzeugung* die erforderlichen Angaben ein.
- Klicken Sie auf die Schaltfläche *Erzeugen*, um das Zertifikat zu erzeugen.

  Beim Generieren des neuen Zertifikats werden alle bestehenden HTTPS-Verbindungen geschlossen, und der HTTPS Server wird automatisch neu gestartet. Je nach Schlüssellänge kann bis zu 5 Minuten dauern.

  Ein expliziter Neustart des iRMC ist **nicht** erforderlich.

## 7.7.6 iRMC S4 Firmware Aktualisierung

Mit der Seite *iRMC S4 Firmware Aktualisierung* können Sie die Firmware des iRMC online aktualisieren. Hierfür stellen Sie das aktuelle Firmware-Image wahlweise lokal am Remote-Arbeitplatz oder auf einem TFTP-Server bereit.

Außerdem erhalten Sie Informationen zur iRMC-Firmware und können den Firmware-Selektor setzten.

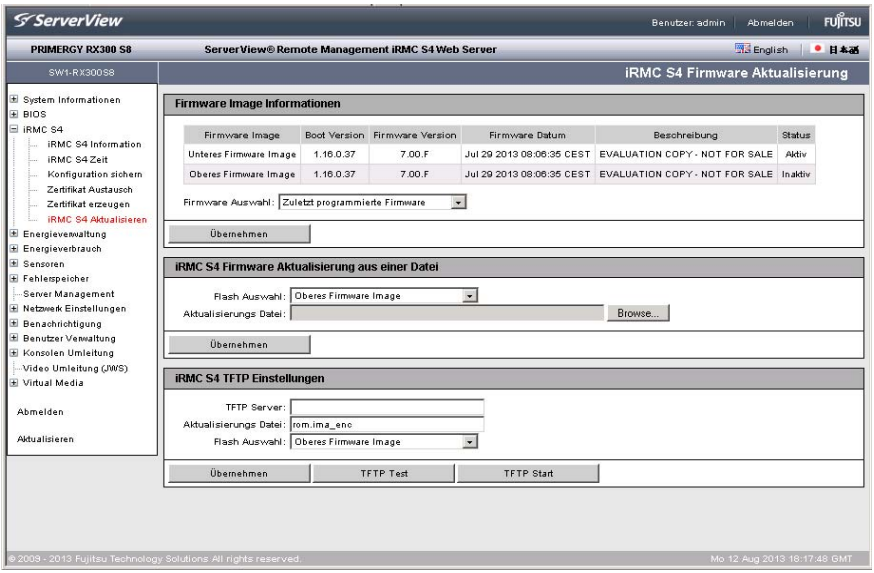



Bild 109: Seite iRMC S4 Aktualisierung

### Firmware Image Informationen

Unter *Firmware Image Information* können Sie Informationen zu Firmware- und SDRR-Version des iRMC einsehen sowie den Firmware-Selektor setzen.

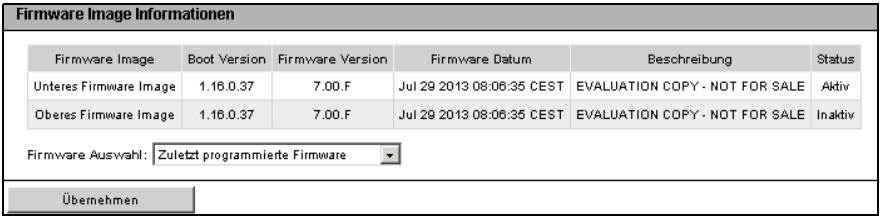



Bild 110: Seite iRMC S4 Firmware Aktualisierung - Firmware Informationen

*Firmware Auswahl*

Mithilfe der Firmware-Auswahl (Firmware-Selektor) legen Sie fest, welches Firmware-Image nach dem nächsten Neustart des iRMC aktiv ist.

Sie haben folgende Möglichkeiten:

– *Automatisch - Firmware mit der höchsten Version*

  Es wird automatisch die Firmware mit dem aktuellsten Versionsstand ausgewählt.

– *Unteres Firmware Image*

  Es wird das untere Firmware-Image ausgewählt.

– *Oberes Firmware Image*

  Es wird das obere Firmware-Image ausgewählt.

– *Firmware mit der ältesten Firmware version*

  Es wird die Firmware mit dem ältesten Versionsstand ausgewählt..

– *Zuletzt programmierte Firmware*

  Es wird die zuletzt programmierte Firmware, also die Firmware mit dem aktuellsten Versionsstand ausgewählt.

– *Zuerst programmierte Firmware*

  Es wird die zuerst programmierte Firmware, also die Firmware mit dem ältesten Versionsstand ausgewählt.

*Übernehmen*

Setzt den Firmware-Selektor auf die unter *Firmware Auswahl* gewählte Einstellung.

### Firmware Aktualisierung aus einer Datei

Mit der Gruppe *Firmware Aktualisierung aus Datei* können Sie die Firmware des iRMC online aktualisieren. Hierfür stellen Sie das aktuelle Firmware-Image in einer Datei auf dem Remote-Arbeitsplatz bereit.

Das zu Ihrem PRIMERGY Server passende Firmware-Image finden Sie auf der ServerView Suite DVD 2 bzw. zum Herunterladen unter *http://support.ts.fujitsu.com/com/support/downloads.html*.

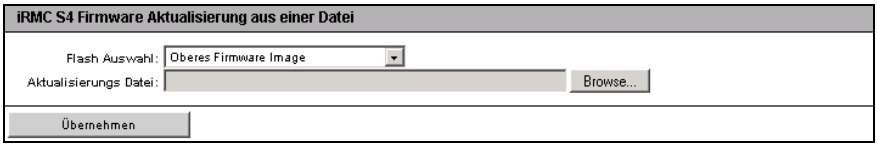



Bild 111: Seite iRMC S4 Firmware Aktualisierung - Aktualisierung aus Datei

*Flash Auswahl*

Hier geben Sie an, welche Firmware des iRMC S2/S3 aktualisiert werden soll.

Sie haben folgende Möglichkeiten:

– *Automatisch - inaktive Firmware*

  Es wird automatisch die inaktive Firmware aktualisiert.

– *Unteres Firmware Image*

  Es wird das untere Firmware-Image (Firmware-Image 1) aktualisiert.

– *Oberes Firmware Image*

  Es wird das obere Firmware-Image (Firmware-Image 2) aktualisiert.

*Aktualisierungs Datei*

Datei, die das Firmware-Image enthält.

Nur vollständige Firmware-Images bestehend aus einer Firmware-Version **und** einer SDRR-Version können aktualisiert werden (z. B. *RX30S8_07.01F_sdr03.47.bin*).

*Durchsuchen...*

Öffnet den Datei-Browser, über den Sie zur Aktualisierungsdatei navigieren können.

*Übernehmen*

Aktiviert Ihre Einstellungen und startet die Aktualisierung der iRMC-Firmware.

### iRMC S4 TFTP Einstellungen

Mit der Gruppe *iRMC S4 TFTP Einstellungen* können Sie die Firmware des iRMC online aktualisieren. Hierfür stellen Sie das aktuelle Firmware-Image auf einem TFTP-Server bereit.

Das zu Ihrem PRIMERGY Server passende Firmware-Image finden Sie auf der ServerView Suite DVD 2 bzw. zum Herunterladen unter *http://support.ts.fujitsu.com/com/support/downloads.html*.

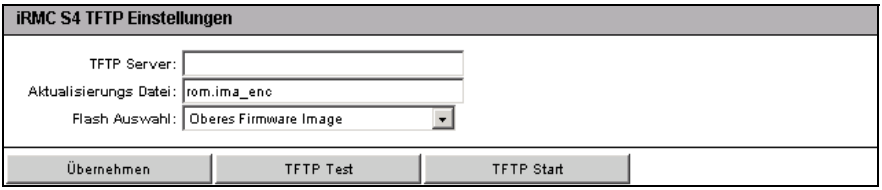



Bild 112: Seite iRMC S4 Firmware Aktualisierung - iRMC S4 TFTP Einstellungen

*TFTP Server*

IP-Adresse oder DNS-Name des TFTP-Servers, auf dem die Datei mit dem BIOS-Image gespeichert ist.

*Aktualisierungs Datei*

Datei, die das Firmware-Image enthält.

Nur vollständige Firmware-Images können aktualisiert werden (z. B. *RX30S8_07.01F_sdr03.47.bin*).

*Flash Auswahl*

Hier geben Sie an, welche Firmware des iRMC S2/S3 aktualisiert werden soll.

Sie haben folgende Möglichkeiten:

– *Automatisch - inaktive Firmware*

  Es wird automatisch die inaktive Firmware aktualisiert.

– *Unteres Firmware Image*

  Es wird das untere Firmware-Image (Firmware-Image 1) aktualisiert.

– *Oberes Firmware Image*

  Es wird das obere Firmware-Image (Firmware-Image 2) aktualisiert.

*Übernehmen*

Übernimmt Ihre Einstellungen.

*TFTP Test*

Testet die Verbindung zum TFTP-Server.

*TFTP Start*

Lädt das Firmware-Image vom TFTP-Server herunterzuladen und startet die Aktualisierung der iRMC-Firmware.

# 7.8 Energieverwaltung

Der Eintrag *Energieverwaltung* enthält die Verweise auf die Seiten für die Energieverwaltung Ihres PRIMERGY Servers:

- "Ein-/Ausschalten - Server ein-/ausschalten" auf Seite 215.
- "Energieverwaltungsoptionen - Energieverwaltung des Servers konfigurieren" auf Seite 220.
- "Netzteil Information - Stromversorgung und IDPROM-Daten der FRU-Komponenten" auf Seite 223.

## 7.8.1 Ein-/Ausschalten - Server ein-/ausschalten

Über die Seite *Ein-/Ausschalten* können Sie den verwalteten Server ein- und ausschalten. Sie werden über die aktuelle Energieversorgung des Servers informiert und können außerdem das Verhalten des Servers beim nächsten Neustart konfigurieren.

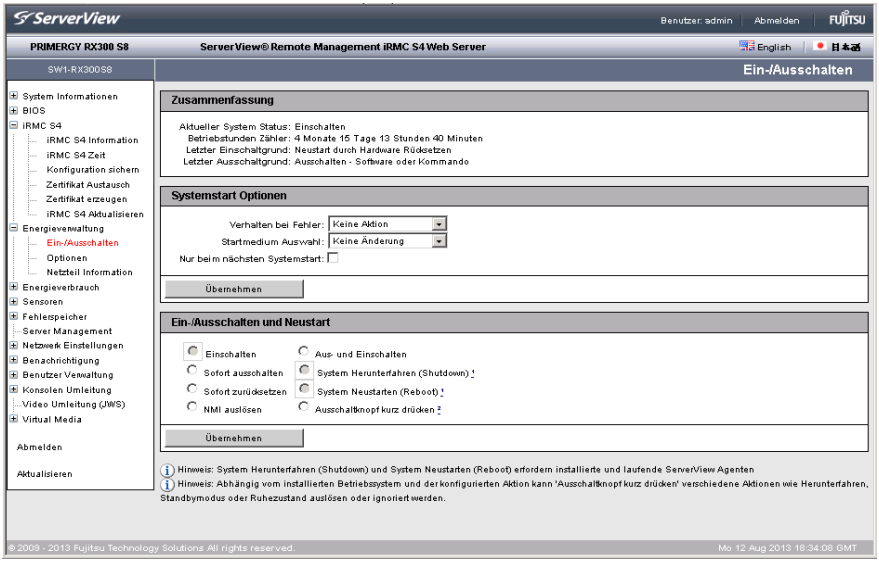



Bild 113: SeiteEin-/Ausschalten

### Zusammenfassung

In der Gruppe *Zusammenfassung* werden Sie über die aktuelle Stromversorgung des Servers sowie über die Ursachen für das zuletzt durchgeführte An- und Abschalten informiert. Außerdem summiert ein Zähler die Monate, Tage und Minuten, die der Server bisher insgesamt eingeschaltet war.

Zusammenfassung
Aktueller System Status: eingeschaltet
Betriebstunden Zähler: 1 Jahre 4 Monate 15 Tage 8 Stunden 55 Minuten
Letzter Einschalt Grund: Neustart nach Warmstart
Letzter Ausschalt Grund: Ausschalten - Ausschalt Knopf

Bild 114: Seite Ein-/Ausschalten - Zusammenfassung

### Systemstart Optionen

Mit der Gruppe *Systemstart Optionen* konfigurieren Sie das Verhalten des Systems bei jedem Neustart des Servers. So können Sie festlegen, von welchem Medium das System gestartet werden soll, und ob das BIOS den Startvorgang unterbrechen soll, wenn während der POST-Phase Fehler auftreten.

Die hier eingestellten Optionen gelten nur für den nächsten Startvorgang. Danach ist wieder der voreingestellte Mechanismus wirksam.

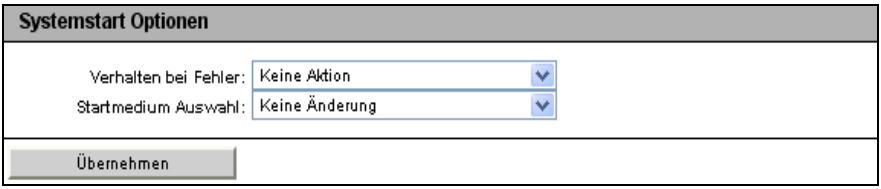



Bild 115: Seite Ein-/Ausschalten - Systemstart Optionen

*Verhalten bei Fehler*

Bestimmt das gewünschte BIOS-Verhalten.

*Keine Aktion*

Startvorgang des Systems fortsetzen, wenn während der POST-Phase Fehler auftreten.

*Bei Fehler anhalten*

Startvorgang des Systems unterbrechen, wenn während der POST-Phase Fehler auftreten.

*Startmedium Auswahl*

Speichermedium, von dem aus der Boot-Vorgang durchgeführt werden soll.

Die folgenden Optionen stehen zur Verfügung:

- *Keine Änderung*: Das System wird von demselben Speichermedium aus wie zuvor gebootet.
- *PXE/iSCSI*: Das System wird über das Netzwerk von PXE/iSCSI gebootet.
- *Festplatte*: Das System wird von der Festplatte aus gebootet.
- *CDROM/DVD*: Das System wird von einer CD/DVD aus gebootet.

– *Diskette*: Das System wird von einer Diskette aus gebootet.

– BIOS Setup: Beim Booten wird das System in das BIOS-Setup geschaltet.

*Boot Type*

Ermittelt den Boot-Modus in dem das System beim nächsten Booten gestartet wird.

Abhängig vom Betriebssystem des Servers, können folgende Optionen ausgewählt werden:

*PC compatible (legacy)*

Das System wird in BIOS-Kompatibilitätsmodus (legacy) gebootet.

*Extensible Firmware Interface Boot (EFI)*

Das System wird in UEFI-Boot-Modus gebootet (nur auf 64-Bit-Betriebssysteme).

*Nur beim nächsten Systemstart*

Die Einstellungen gelten nur für den nächsten Systemstart.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Ein-/Ausschalten und Neustart - Server ein-/ausschalten, neu starten

Mit der Gruppe *Ein-/Ausschalten und Neustart* können Sie den Server ein- und ausschalten oder einen Neustart durchführen.

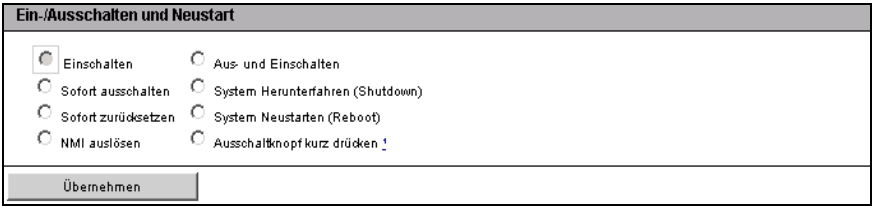



Bild 116: Seite Ein-/Ausschalten - Ein-/Ausschalten und Neustart (Server ist eingeschaltet)

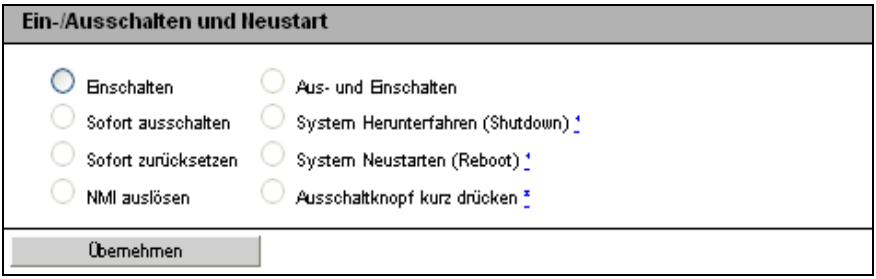



Bild 117: Seite Ein-/Ausschalten - Ein-/Ausschalten und Neustart (Server ist ausgeschaltet)

*Einschalten*
: Schaltet den Server ein.

*Immediate Power Off*
: Schaltet den Server aus unabhängig vom Status des Betriebssystems aus.

*Sofort zurücksetzen*
: Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart).

*NMI auslösen*
: Löst eine nicht-maskierbare Unterbrechung (non-maskable interrupt, NMI) aus Ein NMI ist eine Prozessorunterbrechung, die nicht von Standard-Unterbrechungsmaskierung des Systems ignoriert werden kann.

*Ausschaltknopf kurz drücken*

Abhängig vom installierten Betriebssystem und der konfigurierten Aktion können Sie mit Ausschaltknopf kurz drücken unterschiedliche Aktionen auslösen wie Herunterfahren, Standby-Modus oder Ruhezustand auslösen. Mit diesen Aktionen können Sie den Computer ausschalten oder in den Standby- bzw. Ruhemodus schalten.

*Power Cycle*

Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein. Diese Zeit können Sie im Eingabefeld *Aus-/Einschalt Verzögerung* der Gruppe *ASR&R Einstellungen* (siehe Seite 264) konfigurieren.

*Graceful Power Off (Shutdown)*

System „sanft“ herunterfahren und ausschalten.
Diese Option ist nur verfügbar, wenn die ServerView Agents installiert und beim iRMC als „Connected“ gemeldet sind.

*Graceful Reset (Reboot)*

Graceful Shutdown und Reboot.
Diese Option ist nur verfügbar, wenn die ServerView Agents installiert und beim iRMC als „Connected“ gemeldet sind.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um die gewünschte Aktion zu starten.

## 7.8.2 Energieverwaltungsoptionen - Energieverwaltung des Servers konfigurieren

Über die Seite *Energieverwaltungsoptionen* können Sie das Verhalten des Servers nach Stromausfall und die Ein-/Ausschaltzeiten des Server festlegen.

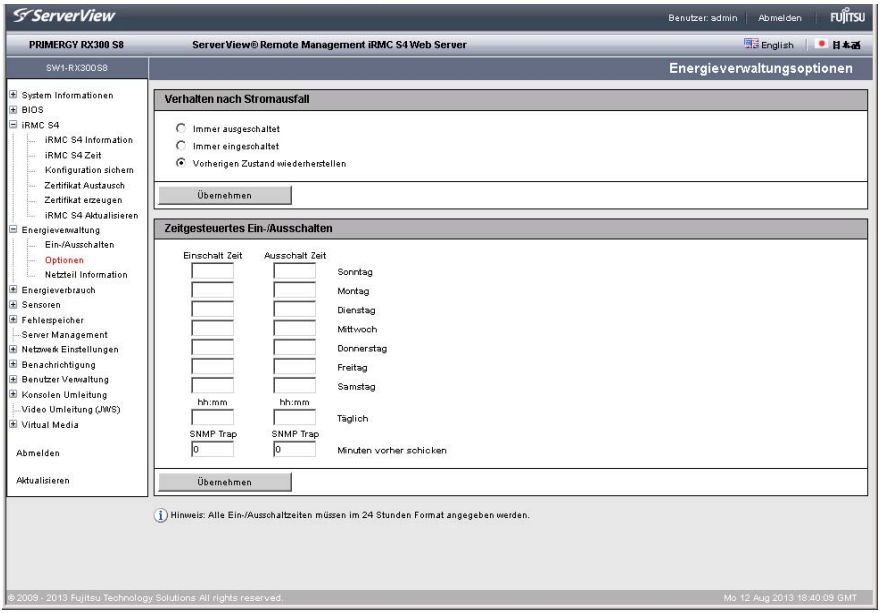



Bild 118: Seite Energieverwaltunsgoptionen:

### Verhalten nach Stromausfall - Verhalten des Servers nach einem Stromausfall festlegen

Mit der Gruppe *Verhalten nach Stromausfall* konfigurieren Sie die Energieverwaltung für den Server nach einem Stromausfall.

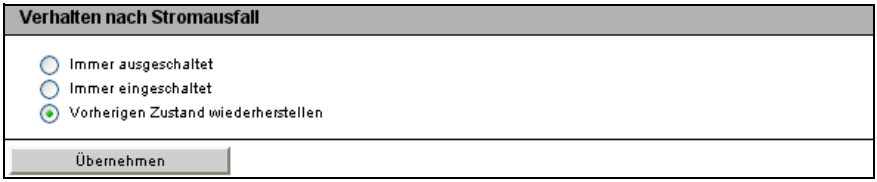



Bild 119: Seite Energieverwaltungsoptionen - Verhalten nach Stromausfall

*Immer ausgeschaltet*
: Nach Stromausfall bleibt der Server immer ausgeschaltet.

*Immer eingeschaltet*
: Nach Stromausfall wird der Server jedesmal wieder eingeschaltet.

*Vorherigen Zustand wiederherstellen*
: Die Energieversorgung des Servers wird auf den Status der Energieversorgung vor dem Stromausfall gesetzt.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Die konfigurierte Aktion wird nach einem Stromausfall ausgeführt.

### Zeitgesteuertes Ein-/Ausschalten - Ein-/Ausschaltzeiten für den Server festlegen

In den Eingabefeldern der Gruppe *Zeitgesteuertes Ein-/Ausschalten* spezifizieren Sie die Ein-/Ausschalt-Zeiten des Servers an den einzelnen Wochentagen oder - einheitlich für alle Wochentage - die täglichen Ein-/Ausschalt-Zeiten.

Die Angaben im Eingabefeld *Täglich* haben Vorrang!

Außerdem können Sie in den Feldern *Trap* festlegen, ob und gegebenenfalls wie viele Minuten vor einem geplanten Ein-/Ausschalten des verwalteten Servers der iRMC S4 einen SNMP-Trap an die Management-Konsole senden soll. Wenn Sie den Wert „0“ angeben, werden keine Traps gesendet.

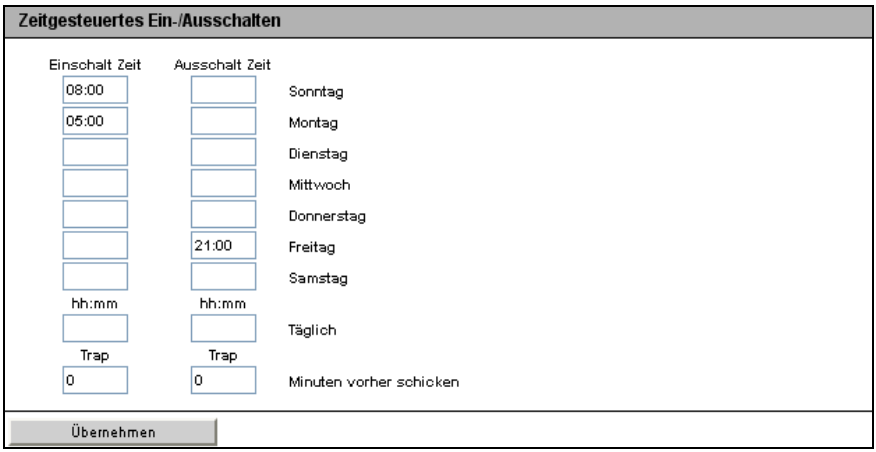



Bild 120: Seite Energieverwaltungsoptionen Zeitgesteuertes Ein-/Ausschalten

## 7.8.3 Netzteil Information - Stromversorgung und IDPROM-Daten der FRU-Komponenten

Auf Seite *Netzteil Information* können Sie sich über die Spezifikationen für die Stromversorgung sowie über die IDPROM-Daten der FRUs des Servers informieren.

In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice) -Funktionalität unterstützt wird.

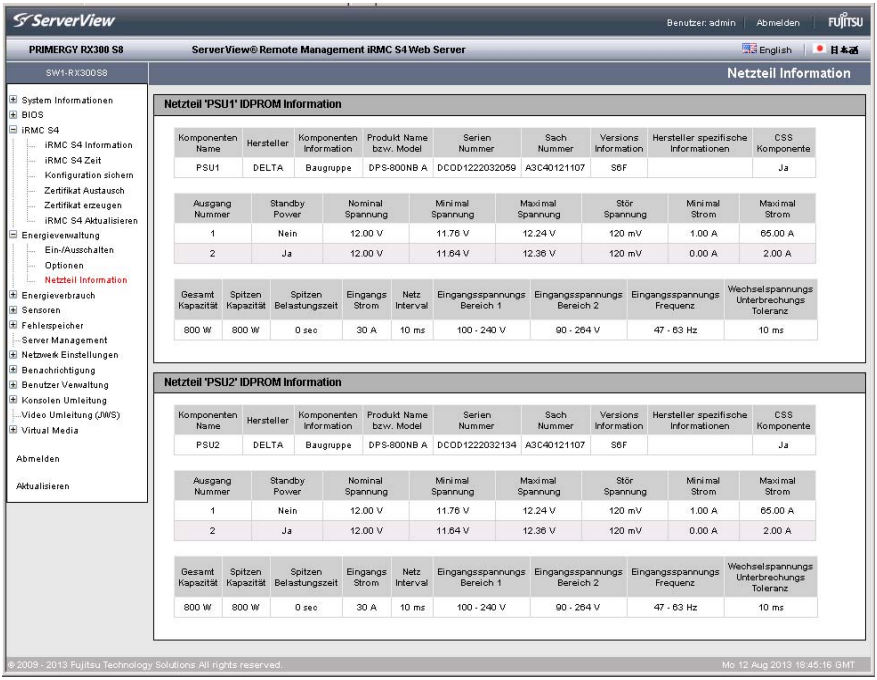

ServerView
Benutzer: admin
Abmelden
FUJITSU
PRIMERGY RX300 S8
ServerView® Remote Management iRMC S4 Web Server
English
日本語
SW1-RX300S8
Netzteil Information
System Informationen
BIOS
iRMC S4
iRMC S4 Information
iRMC S4 Zeit
Konfiguration sichern
Zertifikat Austausch
Zertifikat erzeugen
iRMC S4 Aktualisieren
Energieverwaltung
Ein-/Ausschalten
Optionen
Netzteil Information
Energieverbrauch
Sensoren
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigung
Benutzer Verwaltung
Konsolen Umleitung
Video Umleitung (JWS)
Virtual Media
Abmelden
Aktualisieren
Netzteil 'PSU1' IDPROM Information
Komponenten Name | Hersteller | Komponenten Information | Produkt Name bzw. Model | Serien Nummer | Sach Nummer | Versions Information | Hersteller spezifische Informationen | CSS Komponente
PSU1 | DELTA | Baugruppe | DPS-800NB A | DCOD1222032059 | A3C40121107 | S6F | | Ja
Ausgang Nummer | Standby Power | Nominal Spannung | Minimal Spannung | Maximal Spannung | Stör Spannung | Minimal Strom | Maximal Strom
1 | Nein | 12.00 V | 11.76 V | 12.24 V | 120 mV | 1.00 A | 65.00 A
2 | Ja | 12.00 V | 11.64 V | 12.36 V | 120 mV | 0.00 A | 2.00 A
Gesamt Kapazität | Spitzen Kapazität | Spitzen Belastungszeit | Eingangs Strom | Netz Interval | Eingangsspannungs Bereich 1 | Eingangsspannungs Bereich 2 | Eingangsspannungs Frequenz | Wechselspannungs Unterbrechungs Toleranz
800 W | 800 W | 0 sec | 30 A | 10 ms | 100 - 240 V | 90 - 264 V | 47 - 63 Hz | 10 ms
Netzteil 'PSU2' IDPROM Information
Komponenten Name | Hersteller | Komponenten Information | Produkt Name bzw. Model | Serien Nummer | Sach Nummer | Versions Information | Hersteller spezifische Informationen | CSS Komponente
PSU2 | DELTA | Baugruppe | DPS-800NB A | DCOD1222032134 | A3C40121107 | S6F | | Ja
Ausgang Nummer | Standby Power | Nominal Spannung | Minimal Spannung | Maximal Spannung | Stör Spannung | Minimal Strom | Maximal Strom
1 | Nein | 12.00 V | 11.76 V | 12.24 V | 120 mV | 1.00 A | 65.00 A
2 | Ja | 12.00 V | 11.64 V | 12.36 V | 120 mV | 0.00 A | 2.00 A
Gesamt Kapazität | Spitzen Kapazität | Spitzen Belastungszeit | Eingangs Strom | Netz Interval | Eingangsspannungs Bereich 1 | Eingangsspannungs Bereich 2 | Eingangsspannungs Frequenz | Wechselspannungs Unterbrechungs Toleranz
800 W | 800 W | 0 sec | 30 A | 10 ms | 100 - 240 V | 90 - 264 V | 47 - 63 Hz | 10 ms
© 2009 - 2013 Fujitsu Technology Solutions. All rights reserved.
Mo 12 Aug 2013 18:45:16 GMT

Bild 121: Seite Netzteil Information

# 7.9 Energieverbrauch - Energieverbrauch des Servers steuern

Der Eintrag *Energieverbrauch* enthält die Verweise auf die Seiten zur Steuerung und Kontrolle des Energieverbrauchs des verwalteten Servers:

– "Konfiguration der Energieverbrauchssteuerung - Energieverbrauch des Servers konfigurieren" auf Seite 225.

– "Energieverwaltungsoptionen - Energieverwaltung des Servers konfigurieren" auf Seite 220. (Wird nicht von allen Servern mit iRMC unterstützt.)

– "Energieverbrauch Verlauf - zeitlichen Verlauf des Energieverbrauchs anzeigen" auf Seite 232 (Wird nicht von allen Servern mit iRMC unterstützt.)

## 7.9.1 Konfiguration der Energieverbrauchssteuerung - Energieverbrauch des Servers konfigurieren

Auf der Seite *Konfiguration der Energieverbrauchssteuerung* können Sie den Modus spezifizieren, nach dem der iRMC S4 den Energieverbrauch Ihres PRIMERGY Servers steuert.

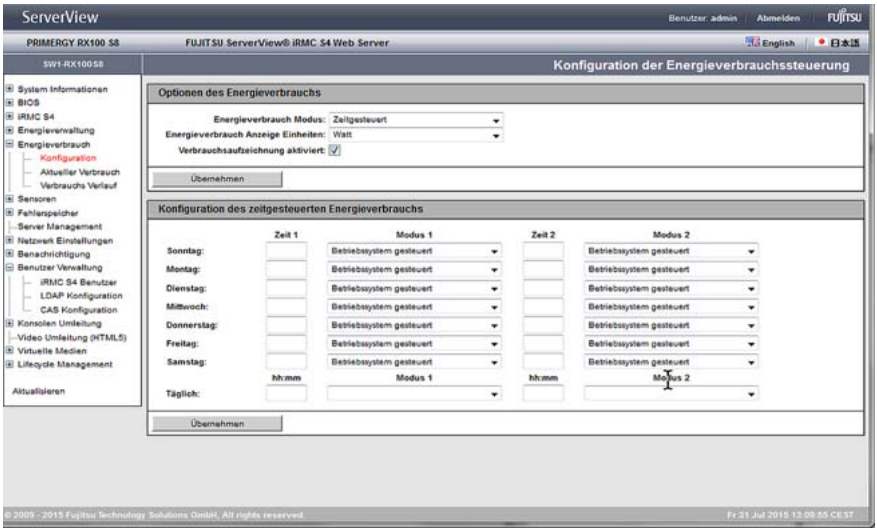



Bild 122: Seite Konfiguration der Enerergieverbrauchssteuerung (nicht zeitgesteuert)

**Voraussetzung:**

Um die Energieverbrauchssteuerung konfigurieren können, müssen folgende Voraussetzungen erfüllt sein:

- Der verwaltete PRIMERGY Server unterstützt dieses Feature.
- Im Menü *Advanced* des BIOS Setup muss *Enhanced Speed Step* oder *Processor Power Management* aktiviert sein.

Wenn Sie unter der Gruppe *Optionen des Energieverbrauchs* oder innerhalb der*Konfiguration des zeitgesteuerten Energieverbrauchs* den Verbrauchsmodus „Begrenzung des Energieverbrauchs“ aktivieren, wird zusätzlich die Gruppe *Begrenzung des Energieverbrauchs* angezeigt (siehe Seite 227).

### Optionen des Energieverbrauchs

In der Gruppe *Optionen des Energieverbrauchs* können Sie den Modus für die Verbrauchssteuerung wählen und festlegen, ob der zeitliche Verlauf des Energieverbrauchs aufgezeichnet werden soll.

*Energieverbrauch Modus*

Modus für die Steuerung des Energieverbrauchs des verwalteten Servers:

- Betriebssystem gesteuert:

  Der Energieverbrauch wird vom Betriebssystem des verwalteten Servers gesteuert.

- *Minimaler Energieverbrauch*:

  Der iRMC steuert den Server im Hinblick auf möglichst geringen Energieverbrauch. In diesem Fall ist die Performance nicht immer optimal.

- *Zeitgesteuert*:

  Der iRMC steuert den Energieverbrauch gemäß eines Zeitplans (siehe "Konfiguration des zeitgesteuerten Energieverbrauchs" auf Seite 227).

- *Begrenzung des Energieverbrauchs*:

  Die Gruppe *Begrenzung des Energieverbrauchs* wird angezeigt (siehe"Optionen der Energieverbrauchsbegrenzung" auf Seite 229).

*Energieverbrauch Anzeige Einheiten*

Einheit der elektrischen Leistung für die Anzeige des Energieverbrauchs:

- *Watt*
- *BTU/h* (British Thermal Unit/hour, 1 BTU/h entspricht 0,293 Watt).

*Verbrauchsaufzeichnung aktiviert*

Wenn Sie diese Option aktivieren, wird der zeitliche Verlauf des Energieverbrauchs aufgezeichnet.

Diese Einstellung ist nur wirksam bei PRIMERGY Servern, die Verbrauchsaufzeichnung unterstützen.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Konfiguration des zeitgesteuerten Energieverbrauchs

Mit der Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* können Sie detailliert die Zeitpläne und Modi (*Betriebssystem gesteuert*, *Minimum Power*, *Verbrauch begrenzen*) festlegen, nach denen der iRMC den Energieverbrauch am verwalteten Server steuert.

Die Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* wird nur dann angezeigt, wenn Sie in der Gruppe *Optionen des Energieverbrauchs* den Verbrauchsmodus *zeitgesteuert* aktiviert haben.

Die Konfiguration des zeitgesteuerten Energieverbrauchs setzt voraus, dass im BIOS Setup die Einstellung *Enhanced Speed Step* aktiviert wurde. Andernfalls wird ein entsprechender Hinweis angezeigt.

Wenn dieser Hinweis trotz aktiviertem „Enhanced Speed Step“ angezeigt wird, kann dies folgende Ursachen haben:

- Die CPU (z.B. Low Power CPU) des Servers unterstützt nicht den zeitgesteuerten Energieverbrauch.
- Das System befindet sich in der BIOS POST-Phase.

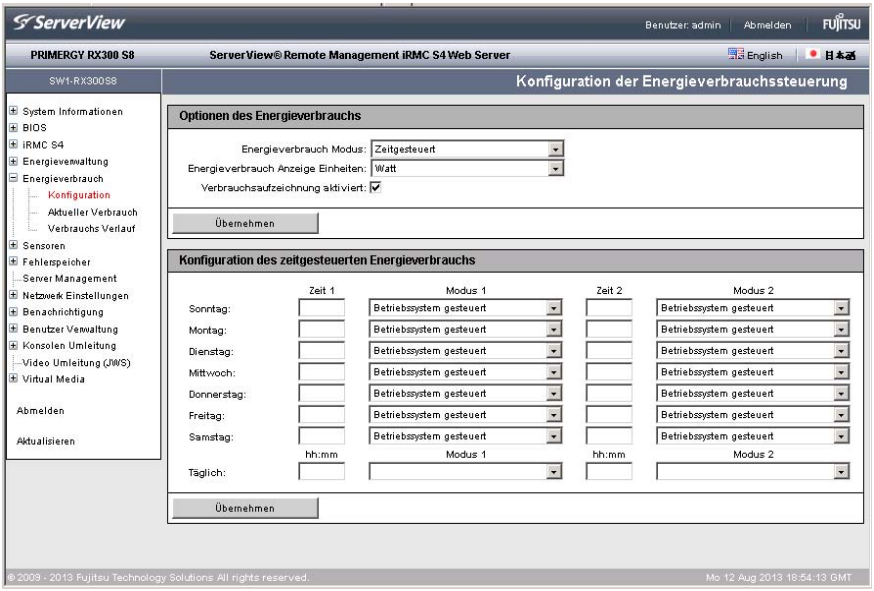



Bild 123: Seite Konfiguration der Energieverbrauchssteuerung (zeitgesteuert)

*Zeit 1*

Zeitpunkt [hh:ss], zu dem der iRMC am zugehörigen Wochentag mit der Verbrauchssteuerung gemäß *Modus 1* startet.

*Zeit 2*

Zeitpunkt [hh:ss], zu dem der iRMC am zugehörigen Wochentag mit der Verbrauchssteuerung gemäß *Modus 2* startet.

*Modus 1*

Verbrauchsmodus, gemäß dem der iRMC die Verbrauchssteuerung am zugehörigen Wochentag ab dem Zeitpunkt *Zeit 1* durchführt.

*Modus 2*

Verbrauchsmodus, gemäß dem der iRMC die Verbrauchssteuerung am zugehörigen Wochentag ab dem Zeitpunkt *Zeit 2* durchführt.

Wählen Sie *Zeit 1* < *Zeit 2*, da andernfalls der unter *Modus 2* festgelegte Verbrauchsmodus erst zu *Zeit 2* am entsprechenden Tag der darauffolgenden Woche aktiviert wird.

Die Angaben bei *Täglich* haben Vorrang!

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Den zeitgesteuerten Energieverbrauch können Sie auch über den Server Configuration Manager konfigurieren (siehe Kapitel "iRMC S4 via Server Configuration Manager konfigurieren" auf Seite 413).

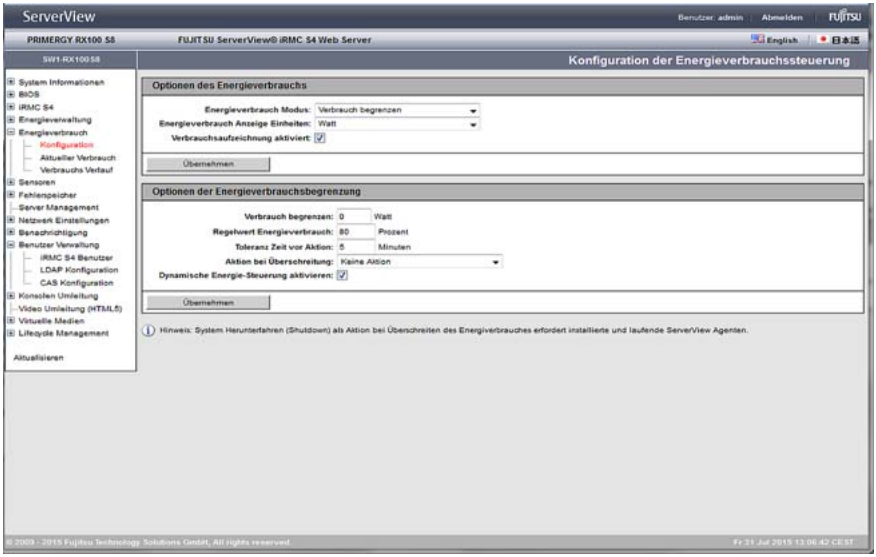
### Optionen der Energieverbrauchsbegrenzung

Die Gruppe *Optionen der Energieverbrauchsbegrenzung* wird in folgenden Fällen angezeigt:

– In der Grupp *Optionen des Energieverbrauchs* ist der Verbrauchsmodus *Begrenzung des Energieverbrauchs* ausgewählt und aktiviert.

– In der Gruppe *Optionen des Energieverbrauchs* ist der Verbrauchsmodus *Zeitgesteuert* aktiviert, und in der Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* ist mindestens einmal der Verbrauchsmodus *Begrenzung des Energieverbrauchs* aktiviert.

  Die Verbrauchsbegrenzung gilt dann für alle Zeitspannen, für die in der Gruppe *Konfiguration des zeitgesteuerten Energieverbrauchs* dieser Verbrauchsmodus aktiviert ist.


ServerView
PRIMERGY RX100 S8
FUJITSU ServerView® iRMC S4 Web Server
Konfiguration der Energieverbrauchssteuerung
Optionen des Energieverbrauchs
Energieverbrauch Modus: Verbrauch begrenzen
Energieverbrauch Anzeige Einheiten: Watt
Verbrauchsaufzeichnung aktiviert:
Übernehmen
Optionen der Energieverbrauchsbegrenzung
Verbrauch begrenzen: 0 Watt
Regelwert Energieverbrauch: 80 Prozent
Toleranz Zeit vor Aktion: 5 Minuten
Aktion bei Überschreitung: Keine Aktion
Dynamische Energie-Steuerung aktivieren:
Übernehmen
Hinweis: System Herunterfahren (Shutdown) als Aktion bei Überschreiten des Energieverbrauches erfordert installierte und laufende ServerView Agenten.
Bild 124: Seite „Konfiguration der Energieverbrauchssteuerung“ (Optionen der Energieverbauchsbegrenzung)

*Verbrauch begrenzen*

Maximale Leistungsaufnahme (in Watt).

Bei Erreichen dieses Werts wird die unter *Aktion bei Überschreitung* festgelegte Aktion ausgeführt. Wenn der Schwellwert überschritten wird, wird eine Warnmeldung in die iRMC S4 SEL geschrieben („CPU Throttlink activated by Power Capping“).

*Regelwert Energieverbrauch*

Der iRMC versucht, den Energieverbrauch auf diesen Wert anzupassen, was als Prozentwert des unter *Verbrauch begrenzen* festgelegten Maximalenergieverbrauchs ausgedrückt wird.

*Überschreitung Toleranz Zeit*

Wartezeit (in Minuten) des Systems, nachdem der Wert *Verbrauch begrenzen* überschritten wurde. Erst danach wird die unter *Aktion bei Überschreitung* festgelegte Aktion ausgeführt.

*Aktion bei Überschreitung*

Aktion, die ausgeführt wird, wenn der Wert von *Verbrauch begrenzen* für mindestens die unter *Überschreitung Toleranz Zeit* festgelegte Dauer überschritten wurde.

*Keine Aktion*

Es wird keine Aktion ausgeführt.

*System Herunterfahren (Shutdown)*

System „sanft“ herunterfahren und ausschalten.

Diese Option wird nur unterstützt, wenn die ServerView Agents installiert und beim iRMC als „Connected“ gemeldet sind.

*Immediate Power Off*

Der Server wird unabhängig vom Status des Betriebssystems sofort ausgeschaltet.

*Dynamische Steuerung aktiviert*

Die Energieverbrauchsbegrenzung wird dynamisch gesteuert. Wenn diese Option aktiviert ist, senkt der iRMC den Energieverbrauch des Servers ab, sobald der Wert für *Verbrauch begrenzen* überschritten wird. Der iRMC versucht, den Energieverbrauch auf das unter *Regelwert Energieverbrauch* festgelegte Niveau anzupassen

## 7.9.2 Aktueller System Energieverbrauch - aktuellen Energieverbrauch anzeigen

Diese Anzeige wird nicht von allen PRIMERGY Servern mit iRMC unterstützt.

Auf der Seite *Aktueller Energieverbrauch* wird der aktuelle Stromverbrauch der Systemkomponenten sowie des Gesamtsystems angezeigt.

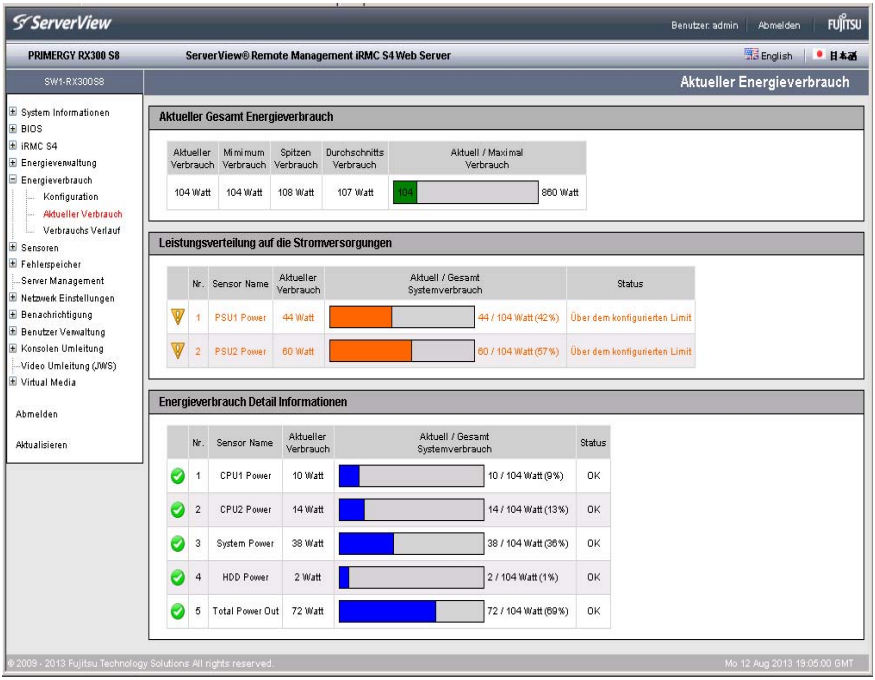


Bild 125: Seite Aktueller Energieverbrauch

## 7.9.3 Energieverbrauch Verlauf - zeitlichen Verlauf des Energieverbrauchs anzeigen

Auf der Seite *Energieverbrauch Verlauf* können Sie sich den zeitlichen Verlauf des Energieverbrauchs Ihres PRIMERGY Servers grafisch anzeigen lassen.

Diese Anzeige wird nicht von allen PRIMERGY Servern mit iRMC S4 unterstützt.

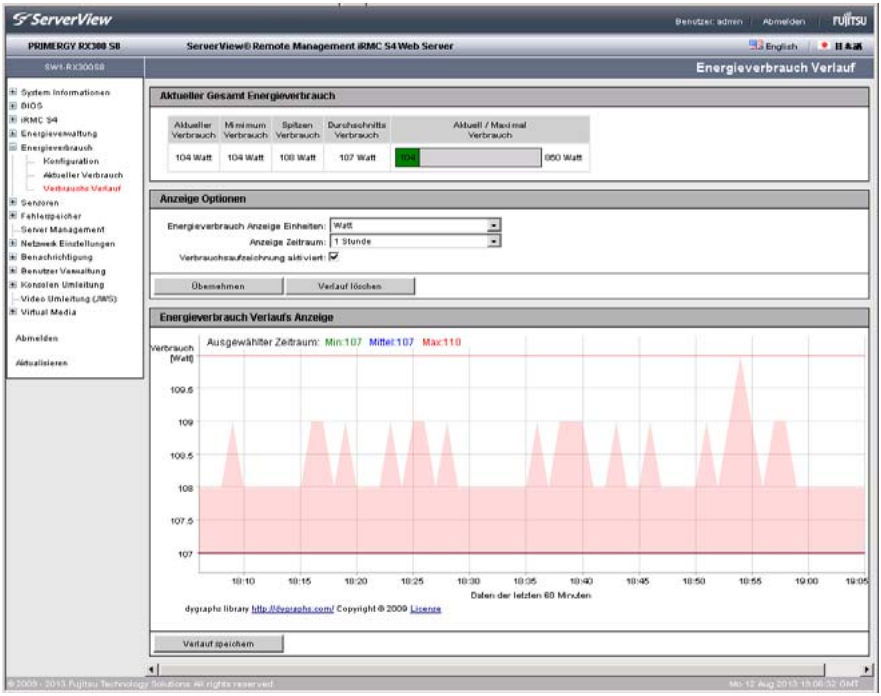



Bild 126: Seite Energieverbrauch Verlauf

### Aktueller Gesamt Energieverbrauch

Diese Option wird nicht für alle PRIMERGY Server unterstützt.

Unter *Aktueller Gesamt Energieverbrauch* werden die Messwerte zum aktuellen, minimalen, maximalen sowie durchschnittlichen Energieverbrauch des verwalteten Servers im aktuellen Intervall angezeigt.

In einer grafischen Anzeige wird außerdem der aktuelle Energieverbrauch des Servers der maximal möglichen Leistungsaufnahme gegenübergestellt.

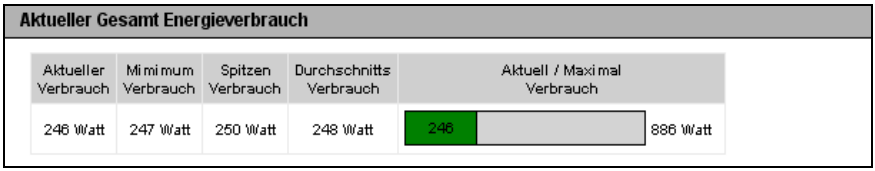



Bild 127: Seite Energieverbrauch Verlauf - Aktueller Gesamt Energieverbrauch

### Anzeige Optionen

Unter Anzeige Optionen spezifizieren Sie die Parameter für die Anzeige des Energieverbrauchsverlaufs.

Bild 128: Seite Energieverbrauch Verlauf -Anzeige Optionen

*Energie Verbrauch Anzeige Einheiten*

Einheit der elektrischen Leistung.

- Watt
- *BTU/h* (British Thermal Unit/hour, 1 BTU/h entspricht 0,293 Watt).

*Anzeige Zeitraum*

Zeitintervall, für das der Leistungsverbrauch grafisch dargestellt wird.

Folgende Intervalle stehen zur Auswahl:

*1 Stunde*

Voreinstellung.
Die Messwerte der letzten Stunde (60 Werte). Da jede Minute ein Messwert erzeugt wird, werden somit alle Messwerte der letzten Stunde angezeigt.

*12 Stunden*

Die Messwerte der letzten 12 Stunden. Es wird ein Messwert pro einem Zeitabschnitt von fünf Minuten dargestellt (jeder 5. Messwert, insgesamt 144 Werte).

*1 Tag*

Die Messwerte der letzten 24 Stunden. Es wird ein Messwert pro einem Zeitabschnitt von 10 Minuten dargestellt (jeder 10. Messwert, insgesamt 144 Werte).

*1 Woche*

Die Messwerte der letzten Woche. Es wird ein Messwert pro Stunde dargestellt (jeder 60. Messwert, insgesamt 168 Werte).

*2 Wochen*

Die Messwerte der letzten beiden Wochen. Es wird ein Messwert pro Zeitabschnitt von zwei Stunden dargestellt (jeder 120. Messwert, insgesamt 168 Werte).

*1 Monat*

Die Messwerte des letzten Monats. Es wird ein Messwert pro einem Zeitabschnitt von ungefähr vier Stunden dargestellt (jeder 240. Messwert, insgesamt 180 Werte).

*1 Jahr*

Die Messwerte der letzten 12 Monate. Es wird ein Messwert pro einem Zeitabschnitt von zwei Tagen dargestellt (jeder 2880. Messwert, insgesamt 180 Werte).

*5 Jahre*

Die Messwerte der letzten 5 Jahre. Es wird ein Messwert pro einem Zeitabschnitt von zwei Tagen dargestellt (jeder 2880. Messwert, insgesamt 180 Werte).

*Verbrauchsaufzeichnung aktiviert*

Wenn Sie diese Option aktivieren, wird der zeitliche Verlauf des Energieverbrauchs aufgezeichnet.

Die Energieverbrauchanzeige ist standardmäßig aktiviert.

Diese Einstellung ist nur wirksam bei PRIMERGY Servern, die Verbrauchsaufzeichnung unterstützen.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.
- Zum Löschen der angezeigten Daten klicken Sie auf die Schaltfläche *Verlauf löschen*.

### Energie Verbrauch Verlaufs Anzeige

Unter *Energieverbrauch Verlaufs Anzeige* wird der zeitliche Verlauf des Energieverbrauchs des verwalteten Servers in einem Kurvendiagramm dargestellt (entsprechend den Einstellungen unter *Anzeige Optionen*). Der tatsächlich angefallene Energieverbrauch kann vom angezeigten Energieverbrauch ungefähr 20% abweichen.

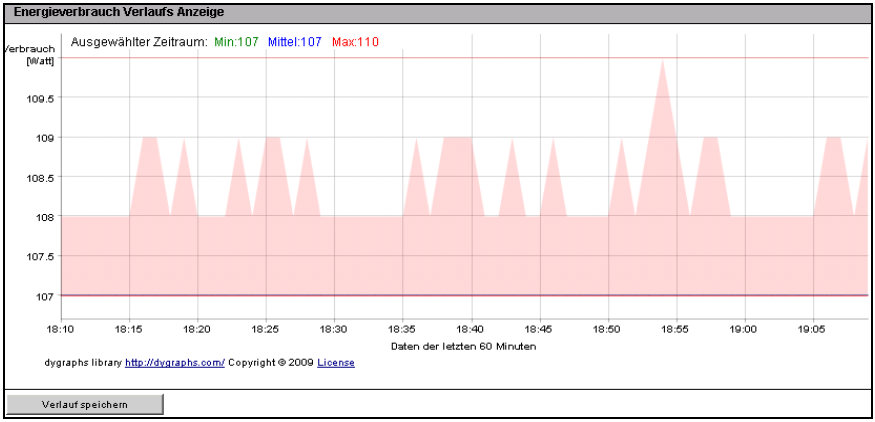



Bild 129: Energieverbrauch Verlauf - Energie Verbrauch Verlaufs Anzeige

# 7.10 Sensoren - Status der Sensoren überprüfen

Unter dem Eintrag „Sensoren“ stehen Ihnen Seiten zur Verfügung, mit denen Sie die Sensoren des verwalteten Servers überprüfen können:

- "Lüfter - Lüfter überprüfen" auf Seite 237.
- "Temperatur - Temperatursensoren überprüfen" auf Seite 240.
- "Spannungen - Spannungssensoren überprüfen" auf Seite 242.
- "Netzteil - Stromversorgung überprüfen" auf Seite 243.
- "Komponenten Status - Status der Serverkomponenten überprüfen" auf Seite 245.

Um die Statusüberprüfung zu erleichtern, wird der Status eines Sensors nicht nur über seinen aktuellen Wert angezeigt, sondern außerdem über Farbcode und Status-Icon:

| | |
|---|---|
| Schwarz / | Der gemessene Wert liegt innerhalb des im Betriebszustand normalen Wertebereichs. |
| Orange / | Der gemessene Wert übersteigt die Warnschwelle. Der Systembetrieb ist aber noch nicht gefährdet. |
| Rot / | Der gemessene Wert übersteigt die kritische Schwelle. Der Systembetrieb kann gefährdet sein und die Datenintegrität könnte bedroht sein. |

Tabelle 7: Status der Sensoren

## 7.10.1 Lüfter - Lüfter überprüfen

Die Seite *Lüfter* informiert über Lüfter und deren Status.

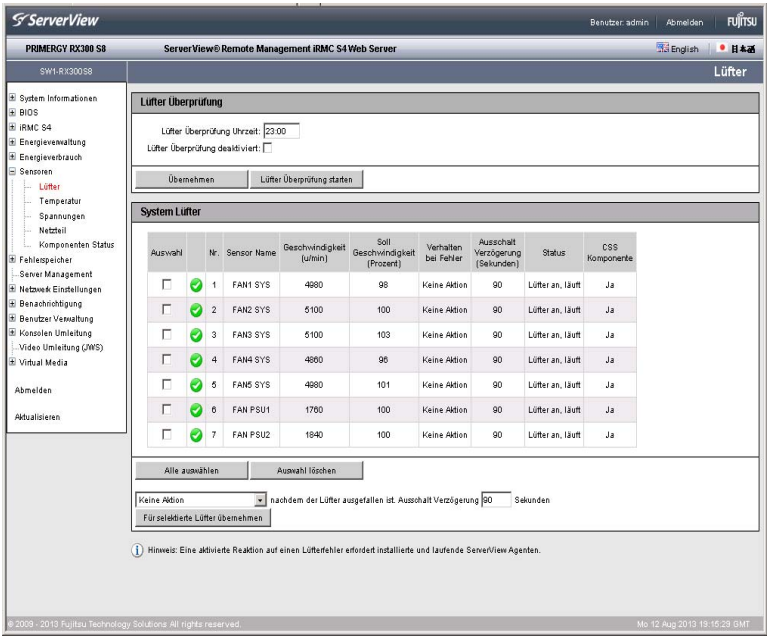


Bild 130: Seite Lüfter

### Lüfter Überprüfung - Lüfter testen

Mit der Gruppe *Lüfter überprüfen* können Sie einen Zeitpunkt für einen automatischen Start der Lüfter-Überprüfung festlegen oder die Überprüfung der Lüfter explizit starten.

Die *Lüfter Überprüfung* führt die Lüfterüberprüfung mit einer annähernden Geschwindigkeit der derzeit erforderlichen durch. Daher ist die Lüfterüberprüfung nicht hörbar.

*Lüftertest Uhrzeit*

Tragen Sie hier den Zeitpunkt für einen automatischen Start der Lüfter-Überprüfung ein.

*Lüfter überprüfung deaktiviert*

Wenn Sie diese Option wählen, ist die Lüfterprüfung deaktiviert.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.
- Klicken Sie auf die Schaltfläche *Überprüfung starten*, wenn Sie die Lüfter-Überprüfung explizit starten wollen.

### System Lüfter - Server-Verhalten bei Ausfall von Lüftern festlegen

Mit der Gruppe *System Lüfter* können Sie sich über den Status der Lüfter informieren. Dabei können Sie via Option oder Schaltfläche einzelne oder alle Lüfter auswählen und festlegen, ob bei Ausfall dieser Lüfter der Server nach einer spezifizierten Anzahl von Sekunden heruntergefahren werden soll.

*Alle auswählen*
: Alle Lüfter werden ausgewählt.

*Auswahl löschen*
: Alle Auswahlmarkierungen werden gelöscht.

- Markieren Sie die Lüfter, für die Sie ein Verhalten im Fehlerfall definieren wollen.
- Definieren Sie das Verhalten im Fehlerfall über die Liste am unteren Ende des Arbeitsbereichs:
  - Wählen Sie *Keine Aktion*, wenn bei Ausfall der ausgewählten Lüfter der der Server nicht heruntergefahren werden soll.
  - Wählen Sie *Herunterfahren und Ausschalten*, wenn bei Ausfall der ausgewählten Lüfter der Server heruntergefahren und ausgeschaltet werden soll.

    Spezifizieren Sie in diesem Fall außerdem im Eingabefeld Ausschalt Verzögerung die gewünschten Zeitspanne (in Sekunden) zwischen dem Ausfall des Lüfters und dem Herunterfahren des Servers.

    *Herunterfahren und Ausschalten* wird bei einem Lüfterausfall ausgeführt, unabhängig davon, ob auf dem verwalteten Server ServerView Agents ausgeführt werden.

    Bei redundanten Lüftern wird der Server erst dann heruntergefahren, wenn mehr als ein Lüfter defekt ist und für diese Lüfter außerdem *Herunterfahren und Ausschalten* eingestellt ist.

► Klicken Sie auf die Schaltfläche *Für selektierte Lüfter übernehmen*, um Ihre Einstellungen für die ausgewählten Lüfter zu aktivieren.

Wenn im BIOS-Setup die Lüfter des verwalteten Servers auf hohe Geschwindigkeit gesetzt sind, werden Sie durch einen Hinweis über diese Einstellung informiert

## 7.10.2 Temperatur - Temperatursensoren überprüfen

Die Seite *Temperatur* informiert über den Status der Temperatursensoren, die die Temperatur an Serverkomponenten wie z. B CPU oder FBD (Fully buffered DIMM) sowie die Umgebungstemperatur messen.

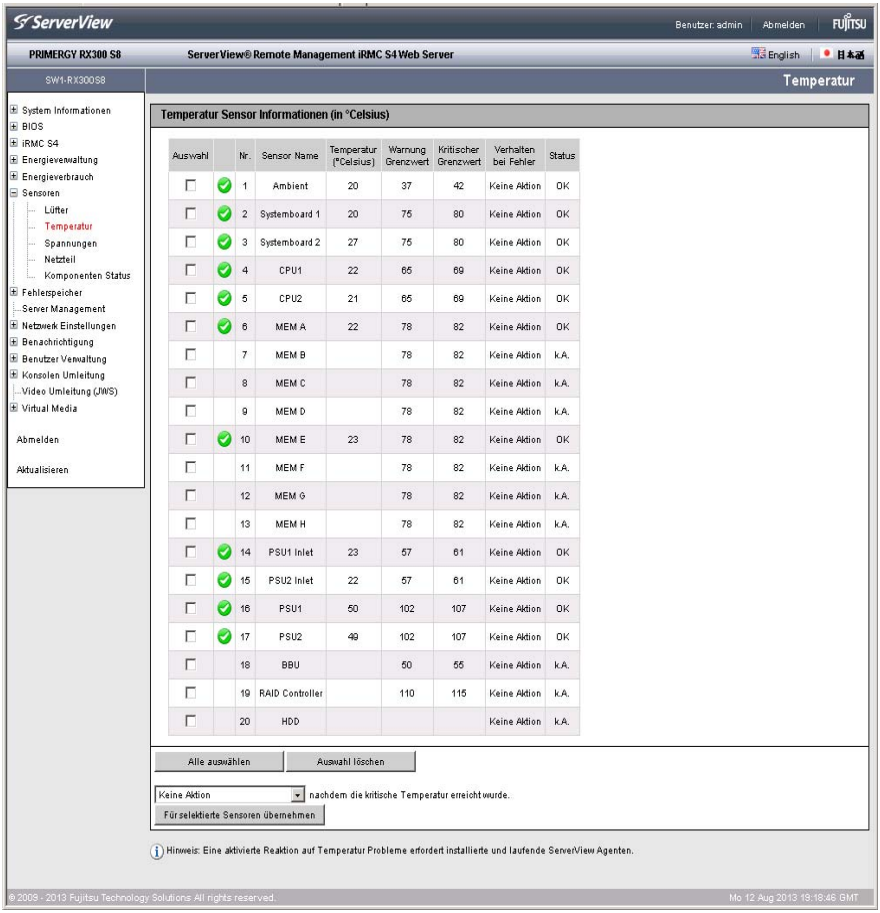

ServerView
Benutzer: admin
Abmelden
FUJITSU
PRIMERGY RX300 S8
ServerView® Remote Management iRMC S4 Web Server
English
SW1-RX300S8
Temperatur
System Informationen
BIOS
iRMC S4
Energieverwaltung
Energieverbrauch
Sensoren
Lüfter
Temperatur
Spannungen
Netzteil
Komponenten Status
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigung
Benutzer Verwaltung
Konsolen Umleitung
Video Umleitung (JWS)
Virtual Media
Abmelden
Aktualisieren
Temperatur Sensor Informationen (in °Celsius)
Auswahl
Nr.
Sensor Name
Temperatur (°Celsius)
Warnung Grenzwert
Kritischer Grenzwert
Verhalten bei Fehler
Status
1 Ambient 20 37 42 Keine Aktion OK
2 Systemboard 1 20 75 80 Keine Aktion OK
3 Systemboard 2 27 75 80 Keine Aktion OK
4 CPU1 22 65 69 Keine Aktion OK
5 CPU2 21 65 69 Keine Aktion OK
6 MEM A 22 78 82 Keine Aktion OK
7 MEM B 78 82 Keine Aktion k.A.
8 MEM C 78 82 Keine Aktion k.A.
9 MEM D 78 82 Keine Aktion k.A.
10 MEM E 23 78 82 Keine Aktion OK
11 MEM F 78 82 Keine Aktion k.A.
12 MEM G 78 82 Keine Aktion k.A.
13 MEM H 78 82 Keine Aktion k.A.
14 PSU1 Inlet 23 57 61 Keine Aktion OK
15 PSU2 Inlet 22 57 61 Keine Aktion OK
16 PSU1 50 102 107 Keine Aktion OK
17 PSU2 49 102 107 Keine Aktion OK
18 BBU 50 55 Keine Aktion k.A.
19 RAID Controller 110 115 Keine Aktion k.A.
20 HDD Keine Aktion k.A.
Alle auswählen
Auswahl löschen
Keine Aktion
nachdem die kritische Temperatur erreicht wurde.
Für selektierte Sensoren übernehmen
Hinweis: Eine aktivierte Reaktion auf Temperatur Probleme erfordert installierte und laufende ServerView Agenten.
© 2009 - 2013 Fujitsu Technology Solutions All rights reserved.
Mo 12 Aug 2013 19:18:46 GMT

Bild 131: Seite Temperatur

Via Option oder Schaltfläche können Sie einzelne oder alle Temperatursensoren auswählen und festlegen, ob bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Server heruntergefahren werden soll.

*Alle auswählen*

Alle Temperatursensoren werden ausgewählt.

*Auswahl löschen*

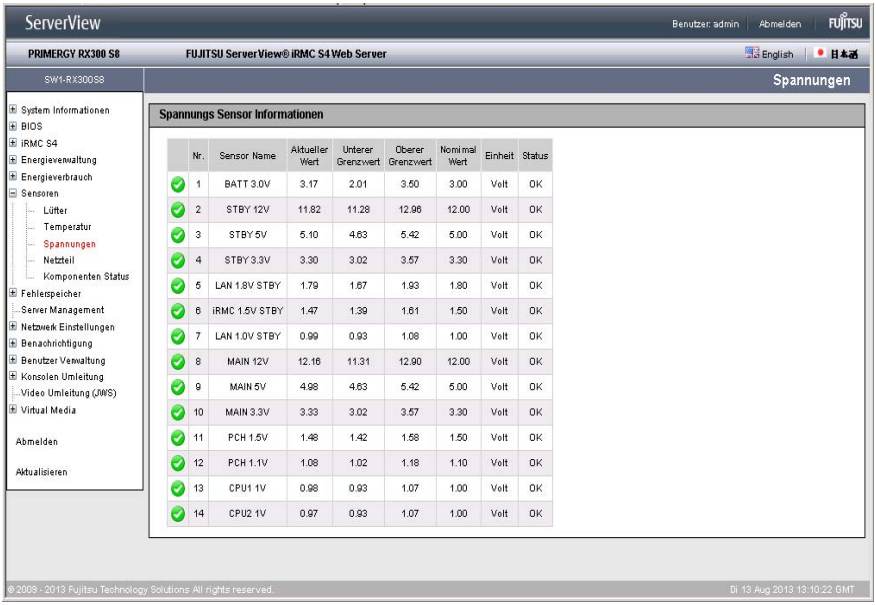
Alle Auswahlmarkierungen werden gelöscht.

- ► Markieren Sie die Sensoren, für die Sie ein Verhalten bei Erreichen der kritischen Temperatur definieren wollen.
- ► Definieren Sie das Verhalten bei Erreichen der kritischen Temperatur über die Liste am unteren Ende des Arbeitsbereichs:
  - – Wählen Sie *Keine Aktion*, wenn bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Shutdown des Servers nicht eingeleitet werden soll.
  - – Wählen Sie *Herunterfahren und Ausschalten*, wenn bei Erreichen der kritischen Temperatur an den ausgewählten Sensoren der Server heruntergefahren und ausgeschaltet werden soll.

    *Herunterfahren und Ausschalten* wird beim Erreichen der kritischen Temperatur ausgeführt, unabhängig davon, ob auf dem verwalteten Server ServerView Agents ausgeführt werden.
- ► Klicken Sie auf die Schaltfläche *Für selektierte Sensoren übernehmen*, um Ihre Einstellungen für die ausgewählten Temperatursensoren zu aktivieren.

## 7.10.3 Spannungen - Spannungssensoren überprüfen

Die Seite *Spannungen* informiert über den Status von Spannungssensoren, die den Serverkomponenten zugeordnet sind.




| Nr. | Sensor Name | Aktueller Wert | Unterer Grenzwert | Oberer Grenzwert | Nominal Wert | Einheit | Status |
|---|---|---|---|---|---|---|---|
| 1 | BATT 3.0V | 3.17 | 2.01 | 3.50 | 3.00 | Volt | OK |
| 2 | STBY 12V | 11.82 | 11.28 | 12.96 | 12.00 | Volt | OK |
| 3 | STBY 5V | 5.10 | 4.63 | 5.42 | 5.00 | Volt | OK |
| 4 | STBY 3.3V | 3.30 | 3.02 | 3.57 | 3.30 | Volt | OK |
| 5 | LAN 1.8V STBY | 1.79 | 1.67 | 1.93 | 1.80 | Volt | OK |
| 6 | iRMC 1.5V STBY | 1.47 | 1.39 | 1.61 | 1.50 | Volt | OK |
| 7 | LAN 1.0V STBY | 0.99 | 0.93 | 1.08 | 1.00 | Volt | OK |
| 8 | MAIN 12V | 12.16 | 11.31 | 12.90 | 12.00 | Volt | OK |
| 9 | MAIN 5V | 4.98 | 4.63 | 5.42 | 5.00 | Volt | OK |
| 10 | MAIN 3.3V | 3.33 | 3.02 | 3.57 | 3.30 | Volt | OK |
| 11 | PCH 1.5V | 1.48 | 1.42 | 1.58 | 1.50 | Volt | OK |
| 12 | PCH 1.1V | 1.08 | 1.02 | 1.18 | 1.10 | Volt | OK |
| 13 | CPU1 1V | 0.98 | 0.93 | 1.07 | 1.00 | Volt | OK |
| 14 | CPU2 1V | 0.97 | 0.93 | 1.07 | 1.00 | Volt | OK |

Bild 132: Seite Spannungen

## 7.10.4 Netzteil - Stromversorgung überprüfen

Die Seite *Netzteil* informiert über den Zustand der Stromversorgung durch die Netzgeräte. Für einige Server-Typen können Sie auf der Seite *Netzteil* außerdem die Einstellungen für die redundante Stromversorgung konfigurieren.

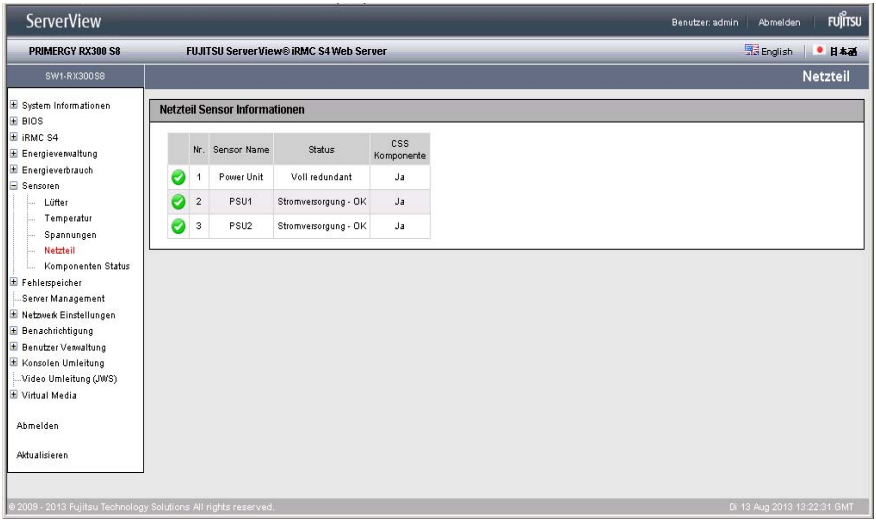



Bild 133: Seite Netzteil

**Unterstützt für iRMC S4**

## Redundante Stromversorgung konfigurieren

Diese Funktionalität kann nur auf Systemen mit mehr als zwei PSUs konfiguriert werden.

In der Gruppe *Konfiguration der redundanten Stromversorgung* können Sie Redundanz-Modus für die Stromversorgung am verwalteten Server einstellen. Welche der nachfolgenden Optionen tatsächlich verfügbar ist, hängt von den Eigenschaften des jeweiligen Servers ab.

*Einfache Redundanz 1 + 1 Ersatz SV*
: Systembetrieb ist garantiert für den Ausfall eines Netzteils bei insgesamt zwei Netzteilen.

*Einfache Redundanz 2 + 1 Ersatz SV*
: Systembetrieb ist garantiert für den Ausfall eines Netzteils bei insgesamt drei Netzteilen.

*Einfache Redundanz 3 + 1 Ersatz SV*
: Systembetrieb ist garantiert für den Ausfall eines Netzteils bei insgesamt vier Netzteilen.

*Phasen Redundanz 2 + 2 (2 Phasen)*
: Zwei der vier Netzteile sind jeweils an eine separate Wechselstromquelle angeschlossen. Dies garantiert die Aufrechterhaltung des Systembetriebs selbst bei Ausfall einer Stromleitung oder eines einzelnen Netzteils.

*Phasen Redundanz 1+ 1 (2 Phasen)*
: Jedes von insgesamt zwei Netzteilen ist an eine separate Wechselstromquelle angeschlossen. Dies garantiert die Aufrechterhaltung des Systembetriebs selbst bei Ausfall einer Stromleitung oder eines einzelnen Netzteils.

## 7.10.5 Komponenten Status - Status der Serverkomponenten überprüfen

Die Seite *Komponenten Status* informiert über den Status der Serverkomponenten: In der Spalte *CSS Komponente* ist für die einzelnen Komponenten vermerkt, ob die CSS (**C**ustomer **S**elf **S**ervice) -Funktionalität unterstützt wird.

Wenn das Servergehäuse geöffnet wird, können die Komponenten mit einer LED mühelos identifiziert werden, indem Sie auf die entsprechende Schaltfläche *Identifizieren* auf der Seite *Komponenten Status* klicken.

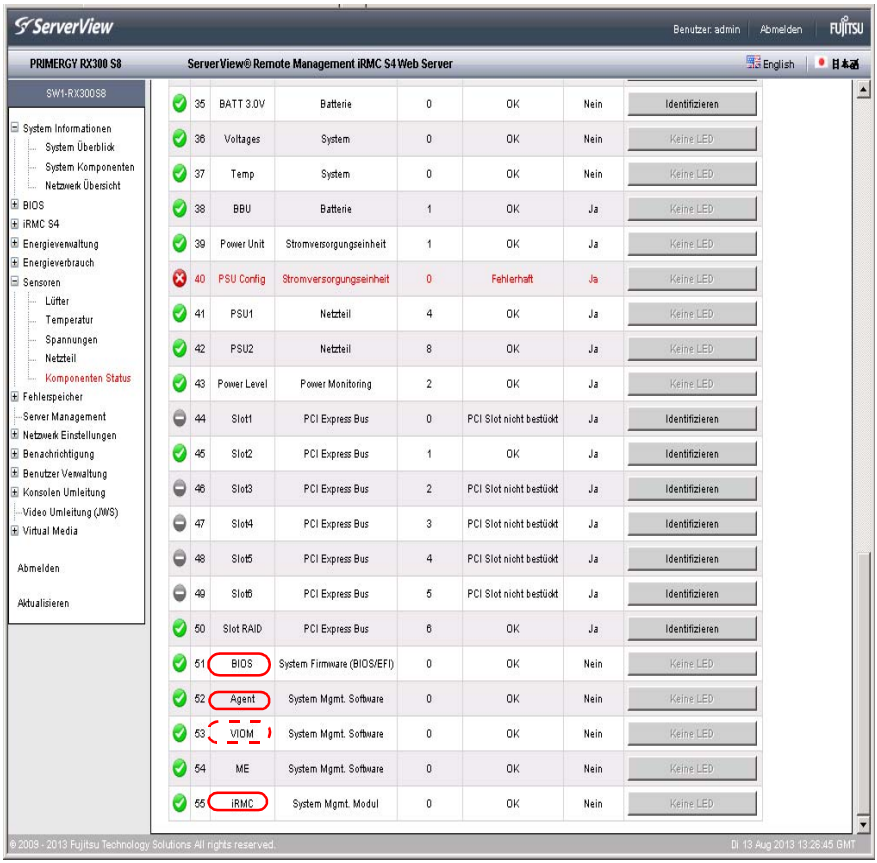

ServerView
Benutzer: admin
Abmelden
FUJITSU
PRIMERGY RX300 S8
ServerView® Remote Management iRMC S4 Web Server
English
SW1-RX300S8
System Informationen
System Überblick
System Komponenten
Netzwerk Übersicht
BIOS
iRMC S4
Energieverwaltung
Energieverbrauch
Sensoren
Lüfter
Temperatur
Spannungen
Netzteil
Komponenten Status
Fehlerspeicher
Server Management
Netzwerk Einstellungen
Benachrichtigung
Benutzer Verwaltung
Konsolen Umleitung
Video Umleitung (JWS)
Virtual Media
Abmelden
Aktualisieren
35 BATT 3.0V Batterie 0 OK Nein Identifizieren
36 Voltages System 0 OK Nein Keine LED
37 Temp System 0 OK Nein Keine LED
38 BBU Batterie 1 OK Ja Keine LED
39 Power Unit Stromversorgungseinheit 1 OK Ja Keine LED
40 PSU Config Stromversorgungseinheit 0 Fehlerhaft Ja Keine LED
41 PSU1 Netzteil 4 OK Ja Keine LED
42 PSU2 Netzteil 8 OK Ja Keine LED
43 Power Level Power Monitoring 2 OK Ja Keine LED
44 Slot1 PCI Express Bus 0 PCI Slot nicht bestückt Ja Identifizieren
45 Slot2 PCI Express Bus 1 OK Ja Identifizieren
46 Slot3 PCI Express Bus 2 PCI Slot nicht bestückt Ja Identifizieren
47 Slot4 PCI Express Bus 3 PCI Slot nicht bestückt Ja Identifizieren
48 Slot5 PCI Express Bus 4 PCI Slot nicht bestückt Ja Identifizieren
49 Slot6 PCI Express Bus 5 PCI Slot nicht bestückt Ja Identifizieren
50 Slot RAID PCI Express Bus 6 OK Ja Identifizieren
51 BIOS System Firmware (BIOS/EFI) 0 OK Nein Keine LED
52 Agent System Mgmt. Software 0 OK Nein Keine LED
53 VIOM System Mgmt. Software 0 OK Nein Keine LED
54 ME System Mgmt. Software 0 OK Nein Keine LED
55 iRMC System Mgmt. Modul 0 OK Nein Keine LED
© 2009 - 2013 Fujitsu Technology Solutions All rights reserved.
Di, 13 Aug 2013 13:26:45 GMT

Bild 134: Seite Komponenten Status

*Identifizieren*

Die mit der entsprechenden Serverkomponente verbundene LED leuchtet auf. Die LED-Bezeichnung ändert sich in *Identify Off*. Ein grünes LED-Symbol anstelle des Statussymbols wird in der linken Spalte, der Seite *Komponenten Status* angezeigt.

Wenn eine Serverkomponente keine LED hat wird die Schaltfläche *Identifizieren* ausgegraut und erhält die Bezeichnung *Keine LED*.

*Identify Off*

Die mit der entsprechenden Serverkomponente verbundene LED wird ausgeschaltet. Die LED-Bezeichnung ändert sich in *Identifizieren*. Das grüne LED-Symbol in der linken Spalte der Seite *Komponenten Status* wird ausgeblendet und das Statussymbol wird erneut gezeigt.

### Einträge mit Sensor Name "iRMC", "Agent", "BIOS", oder "VIOM"

Einträge mit *Sensor Name* „iRMC“, „Agent“, „BIOS“ oder „VIOM“ weist darauf hin, dass iRMC S4, Agent oder BIOS einen Fehler entdeckt haben. Es bedeutet nicht, dass iRMC S4, Agent, BIOS oder VIOM selbst fehlerhaft sind.

### Einträge mit Sensor Name "HDD" und "HDD<n>", "PCIeSSD<n>", "agentless" HDD Monitoring ("out-of-band" HDD Monitoring)

Einträge mit *Sensor Name* "HDD" , "HDD<n>" oder "PCIeSSD<n>" (mit n = 0, 1, 2, ...) zeigen die Status von Festplatten-Laufwerken (Hard Disk Drives, HDD) oder Solid State Disks (SSD) an:

- Der HDD-/SSD-Komponentenstatus wird nur angezeigt, wenn ServerView RAID installiert ist.
- Der Eintrag mit *Sensor Name* "HDD" zeigt den Gesamtstatus über alle HDDs des Servers als Zusammenfassung der Status der einzelnen HDDs an.
- Der HDD-Gesamtstatus des Servers wird von den ServerView Agents und dem ServerView RAID Manager ausgelesen und an den iRMC gemeldet.
- Ein Eintrag mit *Sensor Name* "HDD<n>" oder "PCIeSSD<n> (mit n = 0, 1, 2, ...) zeigt den Status eines einzelnen HDD oder SSD an.

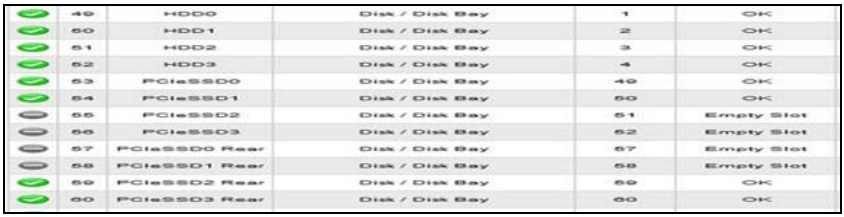
**Beachten Sie:**

– Der iRMC unterstützt diese Funktion nur, wenn die Backplane diese Funktion unterstützt.

– Diese Funktion ist deaktiviert, wenn "RAID Informationen" aktiviert ist.

– Diese Funktionalität wird nur unterstützt, wenn der verwaltete PRIMERGY Server das "agentless" HDD Monitoring (auch "Out-of-band HDD Monitoring" genannt) unterstützt.

Wenn diese Voraussetzungen erfüllt sind, wird der HDD<n>-Status jedes einzelnen HDD direkt, d.h. ohne Nutzung der ServerView Agents an den iRMC S4 gemeldet.



| | | | | | |
|---|---|---|---|---|---|
| | 49 | HDD0 | Disk / Disk Bay | 1 | OK |
| | 50 | HDD1 | Disk / Disk Bay | 2 | OK |
| | 51 | HDD2 | Disk / Disk Bay | 3 | OK |
| | 52 | HDD3 | Disk / Disk Bay | 4 | OK |
| | 53 | PCIeSSD0 | Disk / Disk Bay | 49 | OK |
| | 54 | PCIeSSD1 | Disk / Disk Bay | 50 | OK |
| | 55 | PCIeSSD2 | Disk / Disk Bay | 51 | Empty Slot |
| | 56 | PCIeSSD3 | Disk / Disk Bay | 52 | Empty Slot |
| | 57 | PCIeSSD0 Rear | Disk / Disk Bay | 57 | Empty Slot |
| | 58 | PCIeSSD1 Rear | Disk / Disk Bay | 58 | Empty Slot |
| | 59 | PCIeSSD2 Rear | Disk / Disk Bay | 59 | OK |
| | 60 | PCIeSSD3 Rear | Disk / Disk Bay | 60 | OK |

Bild 135: Statusanzeige für einzelne Festplatten-Laufwerke (HDDs)

– Der HDD-Gesamtstatus des Servers wird von den ServerView Agents und dem ServerView RAID Manager ausgelesen und an den iRMC S4 gemeldet.

Welche Einträge genau in der Tabelle *Komponenten Status Sensor Information* angezeigt werden, hängt deshalb vom Zustand des Servers ab, und ob der Server "agentless" HDD Monitoring unterstützt:

– Der Eintrag mit *Sensor Name* "HDD" zeigt nur dann einen Status in der Spalte *Signal Status* an, wenn die ServerView Agents und der ServerView RAID Manager auf dem verwalteten Server installiert sind und ausgeführt werden. Andernfalls wird stattdessen "N/A" (not available) in der Spalte *Signal Status* angezeigt

– Der HDD- oder SSD-Komponentenstatus wird nicht angezeigt.

– Der Status *Prefail* wird nicht für alle Festplatten unterstützt.

– Die Einträge mit *Sensor Name* "HDD<n>" oder "PCIeSSD<n> (mit n = 0, 1, 2, ...) werden nur angezeigt wenn der verwaltete Server "agentless" HDD Monitoring unterstützt.

# 7.11 Fehlerspeicher und interner Ereignisspeicher

Der Eintrag *Fehlerspeicher* enthält die Verweise auf die Seiten zur Anzeige und Konfiguration des IPMI-Fehlerspeichers (System Eventlog, SEL) und des internen Ereignisspeichers des iRMC S4: Auf einer zusätzlichen Seite können Sie die Syslog-Weiterleitung konfigurieren. Hierbei werden Einträge des Fehlerspeichers und/oder des internen Ereignisspeichers an dedizierte Syslog-Server weitergeleitet. Die folgenden Seiten stehen zur Verfügung:

– "IPMI-Fehlerliste - Information zum Fehlerspeicher und Anzeige der Fehlerspeicher-Einträge" auf Seite 250.

  Die Einträge des internen Fehlerspeichers liefern Informationen zu Audit-Ereignissen (Login-Events, Herstellen einer AVR-Verbindung usw.) sowie zusätzliche Informationen (z.B. IPv6-relevante Informationen und LDAP-Benutzernamen).

– "Interne Ereignisliste - Information zum internen Ereignisspeicher und Anzeige der Einträge" auf Seite 253.

  Die Einträge des IPMI-Fehlerspeichers bieten Informationen zu Ereignissen wie Betriebssystem-Boots/Abschaltvorgänge, Lüfterfehler und iRMC S4-Firmware-Aktualisierungen.

– "Fehlerspeicher Konfiguration - IPMI SEL und internen Ereignisspeicher konfigurieren" auf Seite 256.

– "Syslog Konfiguration – Syslog-Weiterleitung für den Fehlerspeicher und den internen Ereignisspeicher konfigurieren" auf Seite 259.

Zur besseren Übersichtlichkeit sind den einzelnen Ereignis-/Fehlerkategorien farbige Icons zugeordnet:

| | |
|---|---|
| | Kritische |
| | Schwerer Fehler |
| | Leichter Fehler |

Tabelle 8: Ereigniskategorien der Fehlerliste

| | |
|---|---|
| | Information |
| | Customer Self Service (CSS)-Ereignis |

Tabelle 8: Ereigniskategorien der Fehlerliste

## 7.11.1 IPMI-Fehlerliste - Information zum Fehlerspeicher und Anzeige der Fehlerspeicher-Einträge

Die Seite *Fehlerliste* informiert über den IPMI-Fehlerspeicher und zeigt die Einträge des IPMI-Fehlerspeichers) an. Die Einträge des IPMI-Fehlerspeichers bieten Informationen zu Ereignissen wie Betriebssystem-Boots/Abschaltvorgänge, Lüfterfehler und iRMC S4-Firmware-Aktualisierungen.

In der Spalte *CSS Komponente* ist für die einzelnen Ereignisse vermerkt, ob das Ereignis von einer CSS (**C**ustomer **S**elf **S**ervice)-Komponente ausgelöst wurde.

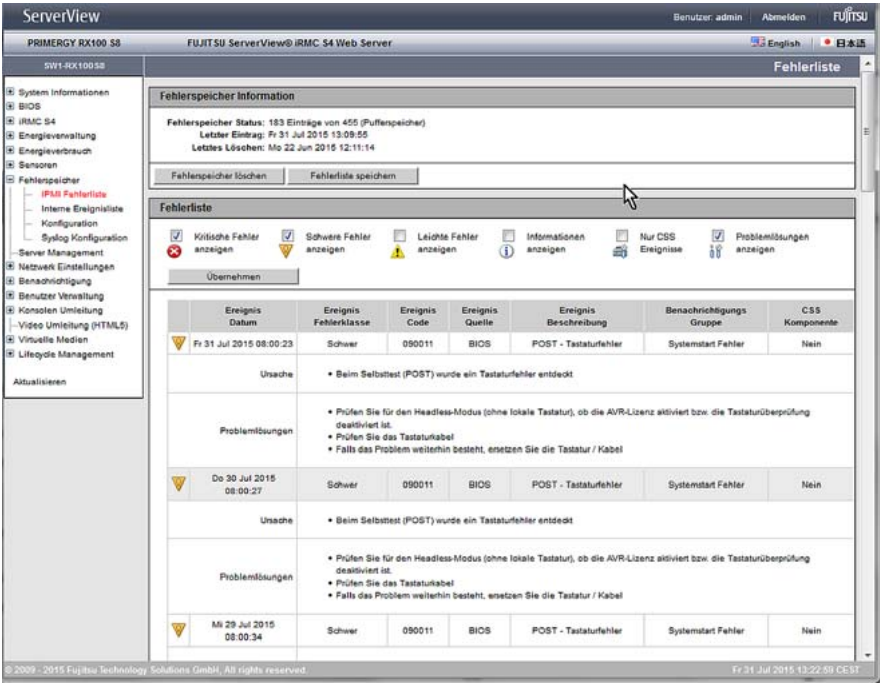



Bild 136: Seite Fehlerliste

### Fehlerspeicher Information

Die Gruppe *Fehlerspeicher Information* informiert über Füllgrad / die Anzahl der Einträge des Fehlerspeichers. Außerdem ist vermerkt, wann zuletzt Einträge hinzugefügt oder gelöscht wurden.

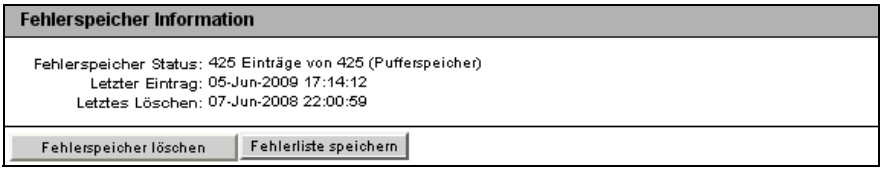



Bild 137: Seite „Fehlerliste“ - Fehlerspeicher Information

*Fehlerspeicher löschen*

Durch Klicken auf *Fehlerspeicher löschen* löschen Sie alle Einträge im Fehlerspeicher.

*Fehlerliste speichern*

Nach dem Klicken auf *Fehlerliste speichern* bietet Ihnen der iRMC S4 die Datei *iRMC S4_EventLog.sel*, in der die Fehlerspeicher-Einträge enthalten sind, zum Herunterladen an.

### IPMI-Fehlerliste

In der Gruppe *Fehlerliste* werden die Fehlerspeicher-Einträge - nach Ereigniskategorien gefiltert - angezeigt.

In der Gruppe *Fehlerliste* können Sie die Filterkriterien für die Dauer der aktuellen Sitzung modifizieren. Die hier vorgenommenen Einstellungen sind jedoch nur bis zum nächsten Abmelden wirksam. Danach gelten wieder die Standardeinstellungen.

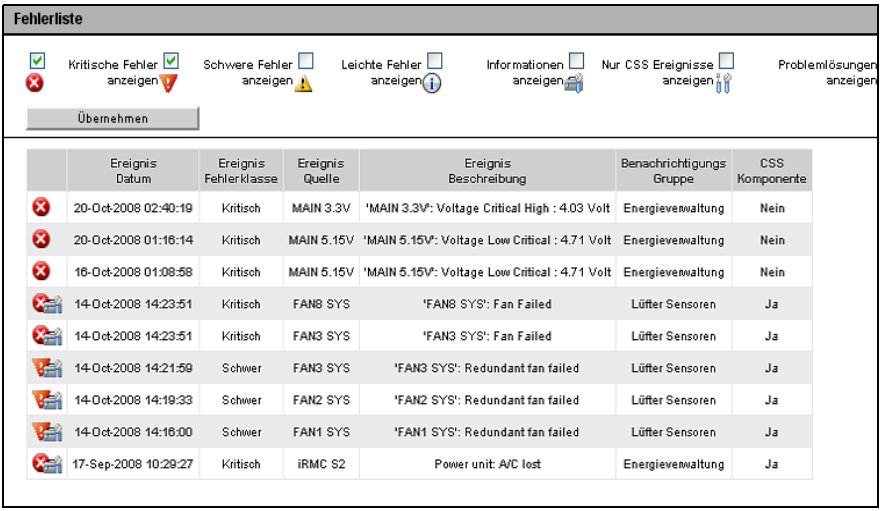

Fehlerliste
Kritische Fehler anzeigen
Schwere Fehler anzeigen
Leichte Fehler anzeigen
Informationen anzeigen
Nur CSS Ereignisse anzeigen
Problemlösungen anzeigen
Übernehmen
Ereignis Datum
Ereignis Fehlerklasse
Ereignis Quelle
Ereignis Beschreibung
Benachrichtigungs Gruppe
CSS Komponente
20-Oct-2008 02:40:19 Kritisch MAIN 3.3V 'MAIN 3.3V': Voltage Critical High : 4.03 Volt Energieverwaltung Nein
20-Oct-2008 01:16:14 Kritisch MAIN 5.15V 'MAIN 5.15V': Voltage Low Critical : 4.71 Volt Energieverwaltung Nein
16-Oct-2008 01:08:58 Kritisch MAIN 5.15V 'MAIN 5.15V': Voltage Low Critical : 4.71 Volt Energieverwaltung Nein
14-Oct-2008 14:23:51 Kritisch FAN8 SYS 'FAN8 SYS': Fan Failed Lüfter Sensoren Ja
14-Oct-2008 14:23:51 Kritisch FAN3 SYS 'FAN3 SYS': Fan Failed Lüfter Sensoren Ja
14-Oct-2008 14:21:59 Schwer FAN3 SYS 'FAN3 SYS': Redundant fan failed Lüfter Sensoren Ja
14-Oct-2008 14:19:33 Schwer FAN2 SYS 'FAN2 SYS': Redundant fan failed Lüfter Sensoren Ja
14-Oct-2008 14:16:00 Schwer FAN1 SYS 'FAN1 SYS': Redundant fan failed Lüfter Sensoren Ja
17-Sep-2008 10:29:27 Kritisch iRMC S2 Power unit: A/C lost Energieverwaltung Ja

Bild 138: Seite „Fehlerliste“, Fehlerliste

*Kritische Fehler anzeigen*, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*, *Nur CSS Ereignisse anzeigen*

Wählen Sie hier gegebenenfalls ein oder mehrere, von der Standardkonfiguration abweichende Fehlerkategorien aus.

*Problemlösungen anzeigen*

Wenn Sie diese Option wählen, wird zu jedem Fehlerspeicher-Eintrag der Fehlerkategorien *Kritischer Fehler* und *Schwerer Fehler* ein Lösungsvorschlag angezeigt.

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen für die Dauer der aktuellen Sitzung zu aktivieren.

## 7.11.2 Interne Ereignisliste - Information zum internen Ereignisspeicher und Anzeige der Einträge

Die Seite *Interner Ereignis Speicher Information* liefert Informationen zum internen Ereignisspeicher und zeigt die zugehörigen Einträge (interne Ereignisliste) an. Der interne Ereignisspeicher umfasst Informationen zu Audit-Ereignissen (Login-Events, Herstellen einer AVR-Verbindung usw.) sowie zusätzliche Informationen (z.B. IPv6-relevante Informationen und LDAP-Benutzernamen).

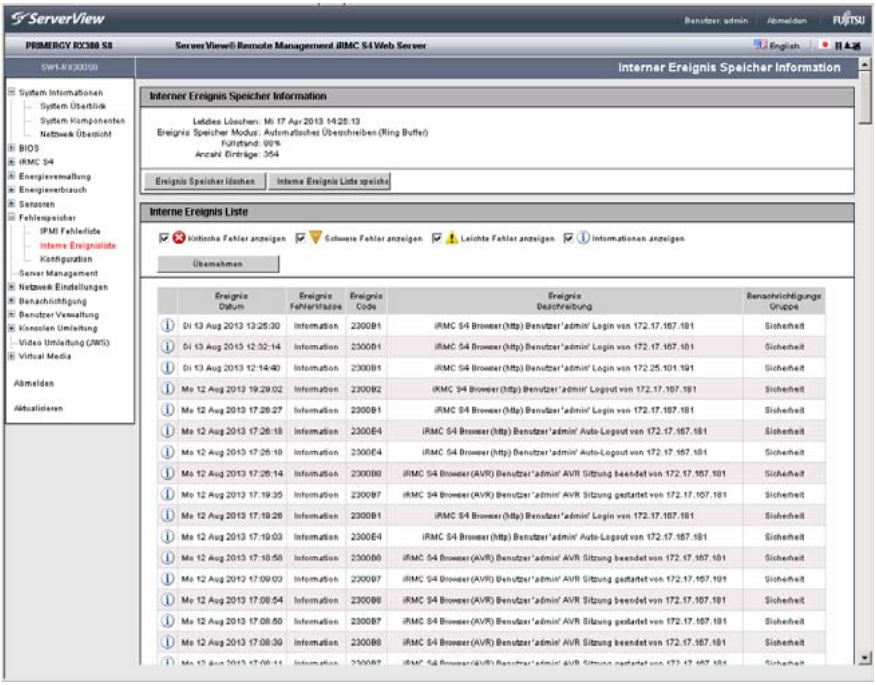



Bild 139: Seite Interner Ereignis Speicher Information

### Interner Ereignis Speicher Information

Die Gruppe *Interer Ereignis Speicher Information* informiert über Füllgrad / die Anzahl der Einträge des internen Ereignisspeichers. Außerdem ist vermerkt, wann zuletzt Einträge hinzugefügt oder gelöscht wurden.

Interner Ereignis Speicher Information
Letztes Löschen: Mi 17 Apr 2013 14:25:13
Ereignis Speicher Modus: Automatisches Überschreiben (Ring Buffer)
Füllstand: 93%
Anzahl Einträge: 374
Ereignis Speicher löschen
Interne Ereignis Liste speiche

Bild 140: Seite „Fehlerliste“ - Fehlerspeicher Information

*Ereignis Speicher löschen*

Durch Klicken auf *Ereignis Speicher löschen* löschen Sie alle Einträge im internen Ereignisspeicher.

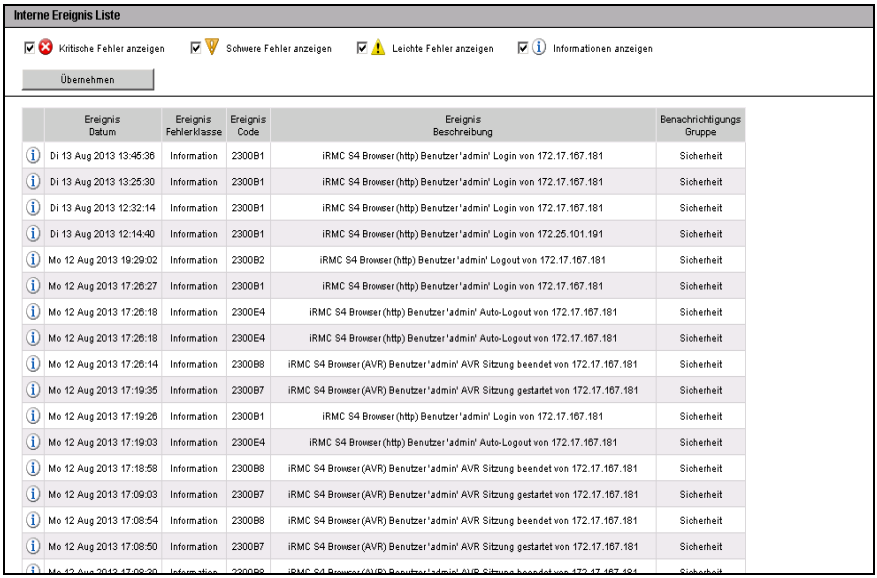
*Interne Ereignis Liste speichern*

Nach dem Klicken auf *Fehlerliste speichern* bietet Ihnen der iRMC S4 die Datei *iRMC S4_InternalEventLog.sel*, in der die Einträge des internen Ereignisspeichers enthalten sind, zum Herunterladen an.

### Interne Ereignisliste

In der Gruppe *Interne Ereignis Liste* werden die Einträge des internen Ereignisspeichers - nach Ereigniskategorien gefiltert - angezeigt.

In der Gruppe *Interne Ereignis Liste* können Sie die Filterkriterien für die Dauer der aktuellen Sitzung modifizieren. Die hier vorgenommenen Einstellungen sind jedoch nur bis zum nächsten Abmelden wirksam. Danach gelten wieder die Standardeinstellungen.




| Ereignis Datum | Ereignis Fehlerklasse | Ereignis Code | Ereignis Beschreibung | Benachrichtigungs Gruppe |
|---|---|---|---|---|
| Di 13 Aug 2013 13:45:36 | Information | 2300B1 | iRMC S4 Browser (http) Benutzer 'admin' Login von 172.17.167.181 | Sicherheit |
| Di 13 Aug 2013 13:25:30 | Information | 2300B1 | iRMC S4 Browser (http) Benutzer 'admin' Login von 172.17.167.181 | Sicherheit |
| Di 13 Aug 2013 12:32:14 | Information | 2300B1 | iRMC S4 Browser (http) Benutzer 'admin' Login von 172.17.167.181 | Sicherheit |
| Di 13 Aug 2013 12:14:40 | Information | 2300B1 | iRMC S4 Browser (http) Benutzer 'admin' Login von 172.25.101.191 | Sicherheit |
| Mo 12 Aug 2013 19:29:02 | Information | 2300B2 | iRMC S4 Browser (http) Benutzer 'admin' Logout von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:26:27 | Information | 2300B1 | iRMC S4 Browser (http) Benutzer 'admin' Login von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:26:18 | Information | 2300E4 | iRMC S4 Browser (http) Benutzer 'admin' Auto-Logout von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:26:18 | Information | 2300E4 | iRMC S4 Browser (http) Benutzer 'admin' Auto-Logout von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:26:14 | Information | 2300B8 | iRMC S4 Browser (AVR) Benutzer 'admin' AVR Sitzung beendet von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:19:35 | Information | 2300B7 | iRMC S4 Browser (AVR) Benutzer 'admin' AVR Sitzung gestartet von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:19:26 | Information | 2300B1 | iRMC S4 Browser (http) Benutzer 'admin' Login von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:19:03 | Information | 2300E4 | iRMC S4 Browser (http) Benutzer 'admin' Auto-Logout von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:18:58 | Information | 2300B8 | iRMC S4 Browser (AVR) Benutzer 'admin' AVR Sitzung beendet von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:09:03 | Information | 2300B7 | iRMC S4 Browser (AVR) Benutzer 'admin' AVR Sitzung gestartet von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:08:54 | Information | 2300B8 | iRMC S4 Browser (AVR) Benutzer 'admin' AVR Sitzung beendet von 172.17.167.181 | Sicherheit |
| Mo 12 Aug 2013 17:08:50 | Information | 2300B7 | iRMC S4 Browser (AVR) Benutzer 'admin' AVR Sitzung gestartet von 172.17.167.181 | Sicherheit |

Bild 141: Seite „Fehlerliste“, Fehlerliste

*Kritische Fehler anzeigen*, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*

Wählen Sie hier gegebenenfalls ein oder mehrere, von der Standardkonfiguration abweichende Fehlerkategorien aus.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen für die Dauer der aktuellen Sitzung zu aktivieren.

## 7.11.3 Fehlerspeicher Konfiguration - IPMI SEL und internen Ereignisspeicher konfigurieren

In der Seite *Fehlerspeicher Konfiguration* können Sie den IPMI-Fehlerspeicher und den internen Ereignisspeicher konfigurieren.

Für jeden der beiden Speicher können Sie festlegen

– welche Einträge in der Seite *Fehlerliste* (siehe Seite 250) bzw. in der *internen Ereignisliste* (siehe Seite 253) standardmäßig angezeigt werden.

– ob der Fehlerspeicher bzw. interne Ereignisspeicher als Ringpuffer oder als linearer Puffer organisiert ist.

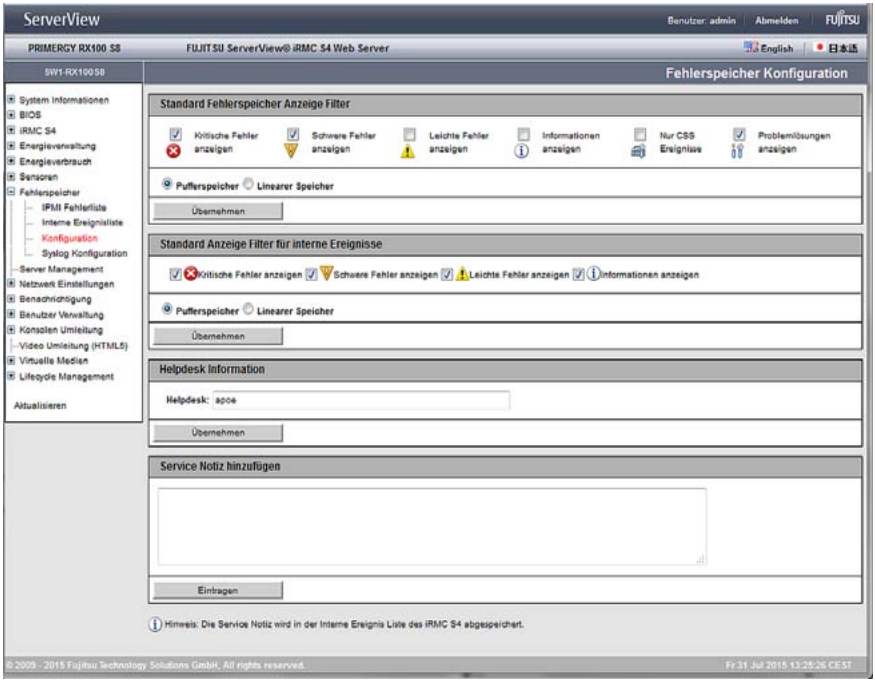


Bild 142: Seite Fehlerspeicher Konfiguration

### Standard Fehlerspeicher Anzeige Filter

*Kritische Fehler anzeigen*, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*, *Nur CSS Ereignisse anzeigen*

Wählen Sie hier eine oder mehrere Fehlerkategorien aus, für die in der Seite *Fehlerliste* standardmäßig die Fehlerspeicher-Einträge angezeigt werden sollen (siehe Seite 250).

*Problemlösungen anzeigen*

Wenn Sie diese Option wählen, wird zu jedem Fehlerspeicher-Eintrag der Fehlerkategorien *Kritischer Fehler*, *Schwerer Fehler* oder *Leichte Fehler* ein Lösungsvorschlag angezeigt.

*Pufferspeicher*

Der Fehlerspeicher wird als Ringpuffer organisiert.

*Linearer Speicher*

Der Fehlerspeicher wird als linearer Puffer organisiert. Wenn der lineare Fehlerspeicher vollständig gefüllt ist, können keine neuen Einträge mehr aufgenommen werden.

*Übernehmen*

Aktiviert Ihre Einstellungen.

### Internen Fehlerspeicher konfigurieren

*Kritische Fehler anzeigen*, *Schwere Fehler anzeigen*, *Leichte Fehler anzeigen*, *Informationen anzeigen*

Wählen Sie hier eine oder mehrere Fehlerkategorien aus, für die in der Seite *Interne Ereignis Liste* standardmäßig die Fehlerspeicher-Einträge angezeigt werden sollen (siehe Seite 253).

*Pufferspeicher*

Der Fehlerspeicher wird als Ringpuffer organisiert.

*Linearer Speicher*

Der Fehlerspeicher wird als linearer Puffer organisiert. Wenn der lineare Fehlerspeicher vollständig gefüllt ist, können keine neuen Einträge mehr aufgenommen werden.

*Übernehmen*

Aktiviert Ihre Einstellungen.

### Helpdesk Information

Bild 143: Helpdesk Information

*Help desk*
String für Helpdesk-Anzeige

*Übernehmen*
Aktiviert Ihre Einstellungen.

### Service Notiz hinzufügen

Im Textfeld der Gruppe *Service Notiz hinzufügen* können Sie eine Service-Notiz eingeben, die in der internen Ereignisliste des iRMC S4 gespeichert wird.

Bild 144: Helpdesk Information

*Übernehmen*
Aktiviert Ihre Einstellungen.

## 7.11.4 Syslog Konfiguration – Syslog-Weiterleitung für den Fehlerspeicher und den internen Ereignisspeicher konfigurieren

Auf der Seite *Syslog Konfiguration* können Sie die Syslog-Weiterleitung konfigurieren. Hierbei werden Ereignisse (Einträge) des Fehlerspeichers und/oder des internen Ereignisspeichers an dedizierte Syslog-Server weitergeleitet.

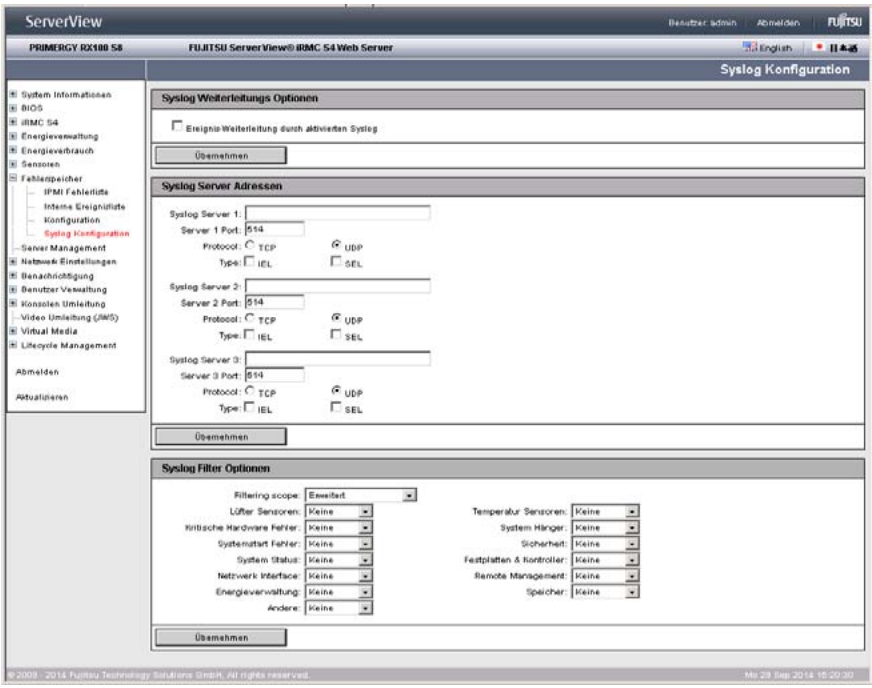


Bild 145: Seite "Syslog Konfiguration"

### Syslog Weiterleitungs Optionen

In der Gruppe *Syslog Weiterleitungs Optionen* können Sie die Syslog-Weiterleitung aktivieren/deaktivieren.

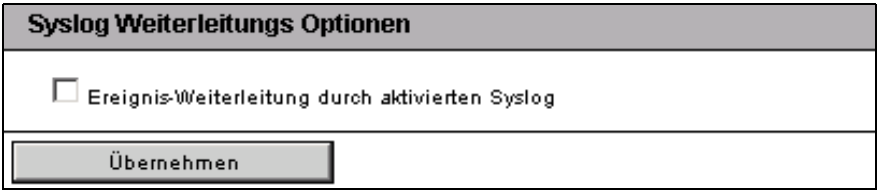



Bild 146: Seite "Syslog Konfiguration" – Syslog Weiterleitungs Optionen

*Ereignis-Weiterleitung durch aktivierten Syslog*
Aktiviert/deaktiviert die Weiterleitung der Ereignisse des Fehlerspeichers und/oder des internen Ereignisspeichers an bis zu drei Syslog-Server mit nachfolgend beschriebener Konfiguration.

### Syslog Server Adressen

In der Gruppe *Syslog Server Adressen* können Sie die Parameter für bis zu drei Syslog-Server konfigurieren.

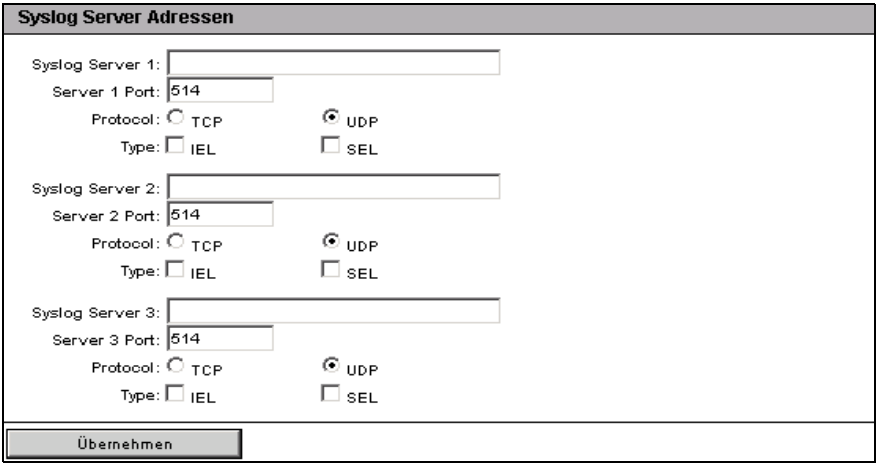



Bild 147: Seite "Syslog Konfiguration" – Syslog Server Adressen

*Server 1*/2/3
IP-Adresse oder DNS-Name des jeweiligen Syslog-Servers.

*Server 1/2/3 Port*

Eingangsanschluss, an dem der Syslog-Server 1/2/3 die weitergeleiteten Ereignisse empfängt.

*Protocol*

Das Protokoll (TCP oder UDP), das für die Übertragung der Ereignisse an den entsprechenden Syslog-Server verwendet wird.

*IEL*

Ereignisse des internen Ereignisspeichers müssen an den entsprechenden Syslog-Server weitergeleitet werden.

*SEL*

Ereignisse des Fehlerspeichers (SEL) müssen an den entsprechenden Syslog-Server weitergeleitet werden.

### Syslog Filter Optionen

In der Gruppe *Syslog Filter Optionen* können Sie die weitergeleiteten Ereignisse nach verschiedenen Kriterien filtern.

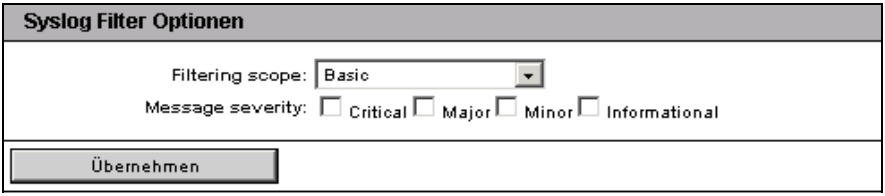



Bild 148: Seite "Syslog Konfiguration" – Syslog Filter Optionen – grundlegende Einstellungen

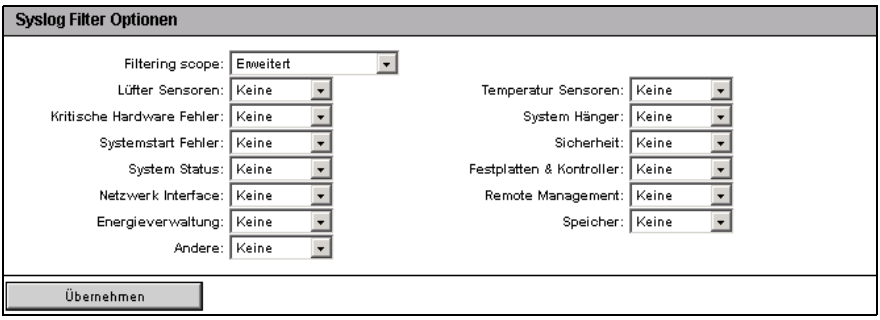



Bild 149: Seite "Syslog Konfiguration" – Syslog Filter Optionen – erweiterte Einstellungen

*Filtering scope*

Legt die Granularität der Filterung fest.

*Grundlegend*

Grundlegende Filterung, bei der nicht zwischen den einzelnen Serverkomponenten, besonderen Ereignissen usw. unterschieden wird.

*Message severity INFORMATIONAL, MINOR, MAJOR, CRITICAL*

Hier können Sie eine oder mehrere Fehlerkategorien auswählen, für die Einträge im Fehlerspeicher an *syslog* weitergeleitet werden sollen (siehe Seite 253).

*Erweitert*

Die Filterung kann separat für alle der folgenden Ereignistypen auf Komponenten- oder Systemebene konfiguriert werden: *Lüfter Sensoren*, *Temperatur Sensoren*, *Kritische Hardware Fehler*, *System Hänger*, *Systemstart Fehler*, *Sicherheit*, *System Status*, *Festplatten & Controller*, *Netzwerk Interface*, *Remote Management*, *Energieverwaltung*, *Speicher* und *Andere*.

Für alle Ereignistypen stehen folgende Optionen zur Verfügung:

*Keine*

Es wird kein Ereignis weitergeleitet.

*Kritische*

Es werden nur Ereignisse mit dem Status *Kritische* weitergeleitet.

*Warnung*

Es werden nur Ereignisse mit dem Status *Kritische* oder *Warnung* weitergeleitet.

*Alle*

Es werden alle Ereignisse weitergeleitet.

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu aktivieren.

# 7.12 Server Management Informationen - Server-Einstellungen konfigurieren

Mithilfe der Seite *Server Management Informationen* können Sie folgende Einstellungen am Server konfigurieren:

– ASR&R-Einstellungen (Automatic Server Reconfiguration and Restart) des Servers (siehe Seite 264)

– Watchdog-Einstellungen (siehe Seite 265)

– Format, in dem das iRMC S4-Gerät die UUID-Informationen zurückgibt (siehe Seite 267)

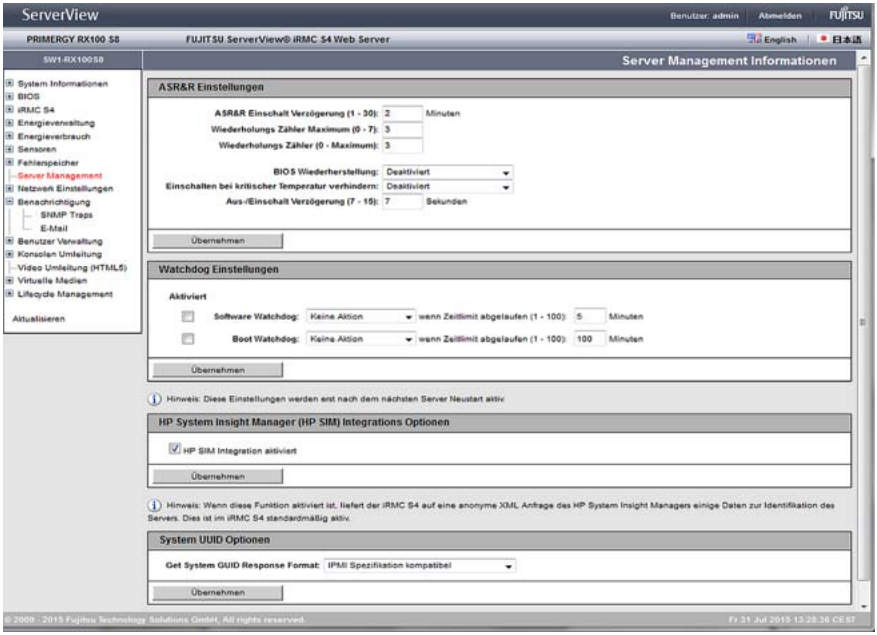


Bild 150: Seite Server Management Information

### ASR&R Einstellungen - ASR&R-Einstellungen konfigurieren

Mit der Gruppe *ASR&R Einstellungen* konfigurieren sie die ASR&R-Einstellungen (Automatic Server Reconfiguration and Restart) des Servers.

Die Einstellungen der Gruppe *ASR&R Einstellungen* sind erst nach dem nächsten Neustart des Servers wirksam.

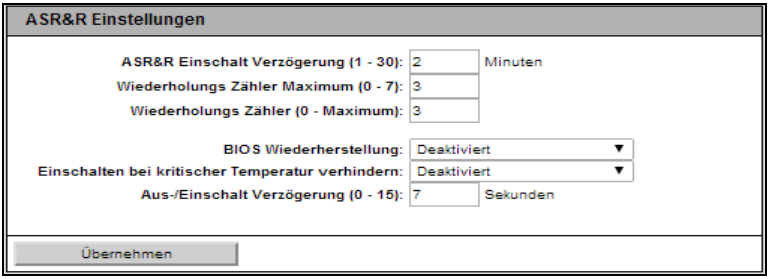



Bild 151: Seite Server Management Informationen - ASR&R Einstellungen

*ASR&R Einschalt Verzögerung (1 - 30)*
Verzögerungszeit (in Minuten), bevor Server neu startet (1 bis 30 Minuten).

*Wiederholungs Zähler Maximum (0 - 7)*
Maximale Anzahl an Neustart-Versuchen, die für den Server nach einem kritischen Fehler möglich sein soll (maximal 7).

*Wiederholungs Zähler (0 - Maximum)*
Anzahl an Neustart-Versuchen, die ein Server nach einem kritischen Fehler unternehmen soll (Maximalwert ist der unter *Wiederholungzähler Maximum* eingestellte Wert).

*BIOS Wiederherstellung*
Das Bit für die BIOS Wiederherstellung (BIOS Recovery Flash Bit) wird aktiviert/deaktiviert:

- *Aktiviert*
  Beim nächsten Starten des Systems wird ein automatischer Flash des BIOS durchgeführt.
- *Deaktiviert*
  Beim nächsten Starten des Systems wird kein automatischer Flash des BIOS durchgeführt.

Die Einstellung *Aktiviert* bietet sich an, wenn nach einer fehlgeschlagenen BIOS-Aktualisierung das Betriebssystem nicht mehr starten kann. Beim nächsten Starten des Systems von der DOS-Diskette (oder einem DOS-Disketten-Image) wird dann das BIOS automatisch wiederhergestellt, d.h. ein BIOS Recovery Flash durchgeführt.

Setzen Sie nach erfolgter BIOS Wiederherstellung die Option BIOS Wiederherstellung wieder auf *Deaktiviert*.

*Prevent Power On on Critical Temperature*

Wenn dies aktiviert ist, wird der Server daran gehindert, im Fall einer kritischen Temperatur eingeschaltet zu werden.

*Aus-/Einschalt Verzögerung (0 - 15)*

Zeitspanne (in Sekunden) zwischen Abschalten und Einschalten während eines automatischen Aus-/Einschalt-Vorgangs (Powercycle).

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu sichern.

  Die konfigurierten Einstellungen werden gespeichert und die konfigurierten Aktionen im entsprechenden Fall ausgeführt.

### Watchdog Einstellungen - Software Watchdog und Boot Watchdog konfigurieren

Mit der Gruppe *Watchdog Einstellungen* können Sie den Software Watchdog und den Boot Watchdog konfigurieren.

Die Einstellungen der Gruppe *Watchdog Einstellungen* sind erst nach dem nächsten Neustart des Servers wirksam.

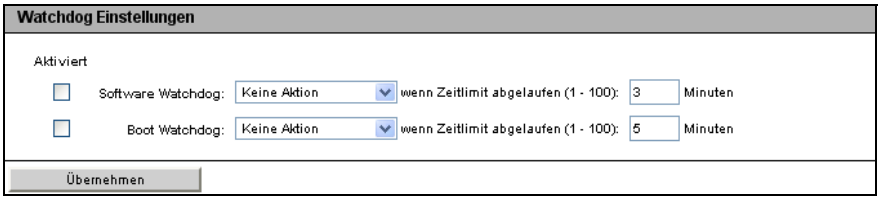



Bild 152: Seite "Server Management Informationen" - Watchdog-Einstellungen

Die **Software Watchdog** überwacht die Arbeit des Systems mithilfe der ServerView Agents. Wenn die ServerView Agents und das Betriebssystem vollständig initialisiert sind, wird der Software Watchdog aktiviert.
Die ServerView Agents kontaktieren in festgelegten Intervallen den iRMC S4.

Laufen von einem ServerView Agents keine Meldungen mehr ein, wird daraus geschlossen, dass das System nicht mehr ordnungsgemäß läuft.
Für diesen Fall können Sie eine Aktion festlegen.

Der **Boot Watchdog** überwacht die Phase zwischen dem Systemstart und dem Zeitpunkt, zu dem die ServerView Agents zur Verfügung stehen.
Wenn die ServerView Agents nicht innerhalb eines festgelegten Zeitraums eine Verbindung zum iRMC S4 des Servers aufbauen, wird daraus geschlossen, dass der Startvorgang nicht erfolgreich verlaufen ist.
Für diesen Fall können Sie eine Aktion festlegen.

Gehen Sie wie folgt vor:

- Aktivieren/Deaktivieren Sie unter *Aktiviert* die Option(en) *Software Watchdog* und/oder *Boot Watchdog*.
- Falls Sie ihn aktiviert haben, wählen Sie hinter *Software Watchdog* und/oder hinter *Boot Watchdog* eine folgende Einstellungen:

  *Keine Aktion*
  Es wird keine Aktion ausgeführt, wenn der Watchdog abgelaufen ist, d. h. der Server läuft weiter. Ein Fehlerspeicher-Eintrag (Eventlog-Eintrag) wird erzeugt.

  *Neustart*
  Die Servermanagement-Software löst einen System-Neustart aus.

  *Power Cycle*
  Der Server wird ausgeschaltet und sofort wieder eingeschaltet.

- Geben Sie nach *wenn Zeitlimit abgelaufen (1 - 100)* die Zeitspanne (in Minuten) an, nach deren Verstreichen diese Aktion ausgeführt werden soll.

  Der Boot Watchdog muss solange warten, bis das System gestartet ist. Vereinbaren Sie deshalb für *wenn Zeitlimit abgelaufen (1 - 100)* eine hinreichend große Zeitspanne.

- Klicken Sie auf die Schaltfläche *Übernehmen*.

  Die konfigurierten Einstellungen werden gespeichert und die konfigurierten Aktionen im entsprechenden Fall ausgeführt.

### HP System Insight Manager (HP SIM) Integrations Optionen

In dieser Gruppe schalten Sie die HP SIM-Integration ein oder aus.

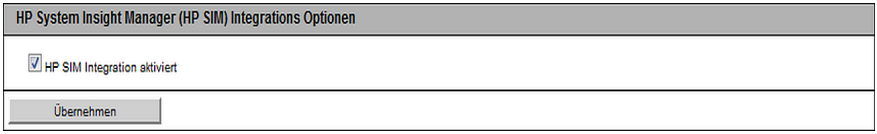



Bild 153: Seite "Server Management Informationen" - HP SIM Optionen

*HP SIM Integration aktiviert*
Schaltet die HP SIM-Integration ein oder aus.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### System UUID-Optionen

In der Gruppe *System UUID Options* können Sie das Format konfigurieren, in dem der iRMC S4 UUID-Information zurückschicken wird.

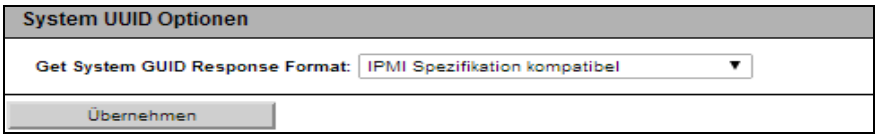



Bild 154: Seite "Server Management Informationen" - System UUID-Optionen

*Get System UUID Response Format*
Format, in dem das iRMC S4-Gerät die UUID-Informationen zurückgibt.

*IPMI Spezifiaktion kompatibel*
System GUID-Antwortformat ist mit der IPMI-Spezifikation kompatibel.

*SMBIOS 2.6-Spezifikation-kompatibel*
System GUID-Antwortformat ist mit der System Management BIOS (SMBIOS)-Referenzspezifikation kompatibel.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

# 7.13 Netzwerk Einstellungen - LAN-Parameter konfigurieren

Der Eintrag *Netzwerk Einstellungen* umfasst die Verweise auf die Seiten, mit denen Sie die LAN-Parameter des iRMC S4 konfigurieren:


– "Netzwerk Schnittstelle - Ethernet-Einstellungen des iRMC S4 konfigurieren" auf Seite 269.

– "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 276.

– "Proxy Einstellungen– Proxyeinstellungen konfigurieren" auf Seite 280.

– "DNS Konfiguration - DNS für den iRMC S4 konfigurieren" auf Seite 282.

– "SNMP Allgemeine Konfiguration" auf Seite 286.

## 7.13.1 Netzwerk Schnittstelle - Ethernet-Einstellungen des iRMC S4 konfigurieren

Mit der Seite *Netzwerk Schnittstelle* können Sie die Ethernet-Einstellungen des iRMC S4 einsehen und ändern.

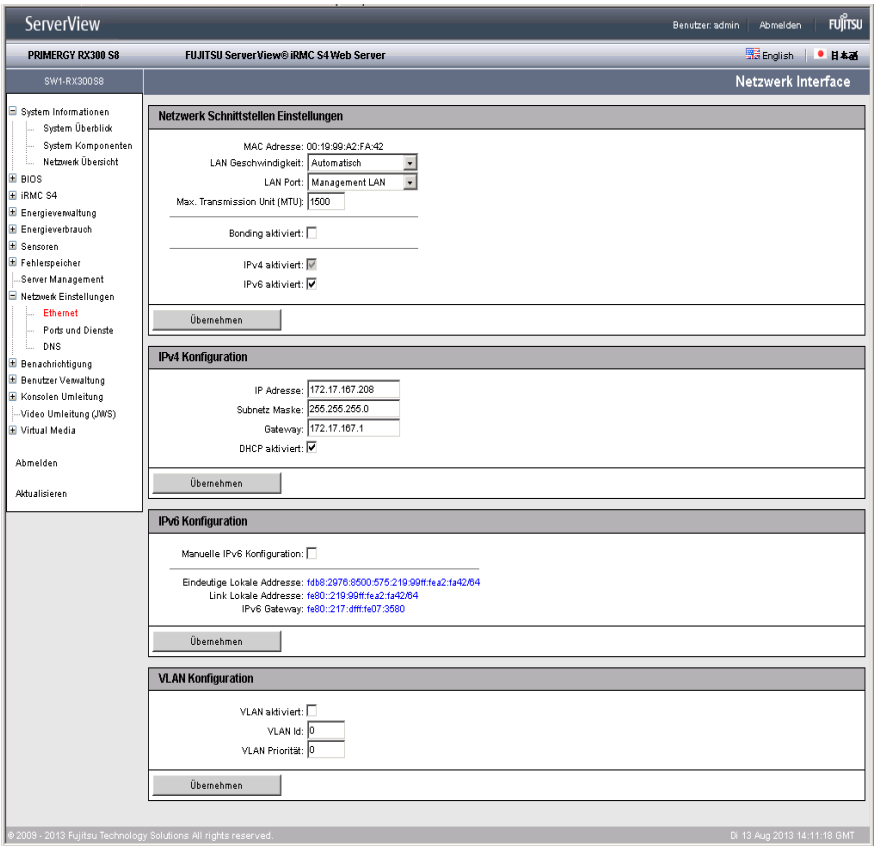


Bild 155: Seite Netzwerk Schnittstelle

**ACHTUNG!**

Kontaktieren Sie den zuständigen Netz-Administrator, bevor Sie Ethernet-Einstellungen ändern.

Wenn Sie für den iRMC S4 unzulässige Ethernet-Einstellungen konfigurieren, ist ein erneuter Zugriff auf den iRMC S4 nur über eine Konfigurationssoftware, über die serielle Schnittstelle oder im BIOS möglich.

Nur Benutzer mit der Berechtigung *iRMC S4 Einstellungen konfigurieren* können Sie Ethernet-Einstellungen editieren (siehe Kapitel "Benutzerverwaltung für den iRMC S4" auf Seite 61).

### Netzwerk Schnittstellen Einstellungen

*MAC Adresse*

Hier wird die MAC-Adresse des iRMC S4 angezeigt.

*LAN Geschwindigkeit*

Diese Option ist deaktiviert/nicht sichtbar, wenn das Netzwerk-Bonding aktiviert ist.

LAN Geschwindigkeit. Zur Auswahl stehen:

- Automatisch
- 1000 MBit/s Voll Duplex (je nach Server-Hardware)
- 100 MBit/s Voll Duplex
- 100 MBit/s Halb Duplex
- 10 MBit/s Voll Duplex
- 10 MBit/s Halb Duplex

Bei *Automatisch* ermittelt der dem iRMC S4 zugeordnete onboard LAN-Controller selbstständig die korrekte Übertragungsgeschwindigkeit und das Duplex-Verfahren des Netzwerkports, an den er angeschlossen ist.

*Max. Transmission Unit (MTU)*

Maximale Paketgröße (in Bytes) der TCP/IP-Datenpakete, die von der TCP/IP-Verbindung akzeptiert werden. (Standard: 3000 Byte).

*LAN Port*

Diese Option ist deaktiviert/nicht sichtbar, wenn das Netzwerk-Bonding aktiviert ist.

Die LAN-Schnittstelle der eingebauten System-NIC (Network Interface Card) kann wahlweise eingerichtet werden als

– Gemeinsames LAN für den „Shared“-Betrieb mit dem System

oder

– Service LAN exklusiv für das Management LAN.

*Bonding aktiviert*

Aktiviert/deaktiviert das Netzwerk-Bonding für den iRMC S4.

Das Netzwerk-Bonding für den iRMC S4 wurde für den Fall eines Ausfalls von Ethernet-Netzwerkadaptern für Redundanz konzipiert. Daher ist der Datenverkehr für das iRMC S4-Netzwerk-Management vor Serviceausfällen geschützt, die beim Ausfall einer einzelnen physischen Verbindung auftreten können.

Der iRMC S4 unterstützt nur den aktiven Backup-Modus, d. h. ein Port ist aktiv, bis die Verbindung ausfällt, dann übernimmt der andere Port die MAC und wird aktiv.

Wenn das Bonding aktiviert ist, werden die Optionen *Aktiver Port*, *LAN Geschwindigkeit* und *LAN Port* deaktiviert bzw. sie sind nicht sichtbar.

Für das iRMC S4-Netzwerk-Bonding müssen sich die betreffenden LAN-Switches in demselben Netzwerk befinden. Darüber hinaus ist keine besondere Switch-Konfiguration für das iRMC S4-Netzwerk-Bonding erforderlich.

**Beachten Sie:**

Wenn dies aktiviert ist, wird das Netzwerk-Bonding ausgesetzt, sobald das Front-LAN aktiviert wird. Der Front-LAN-Port ist aktiviert und ist für die vordefinierte IP-Adresse 192.168.1.1 zugänglich. Wenn dieser Fall eintritt, wird ein entsprechender Hinweis auf der Weboberfläche angezeigt.

Bonding-Einstellungen können dennoch konfiguriert und geändert werden. Die Einstellungen werden übernommen, sobald das Front-LAN deaktiviert wird („link down“), d. h. der Bonding-Modus wird je nach derzeit konfigurierten Bonding-Einstellungen erneut aktiviert.

Die folgende Abbildung zeigt die Funktionsweise des Netzwerk-Bondings:

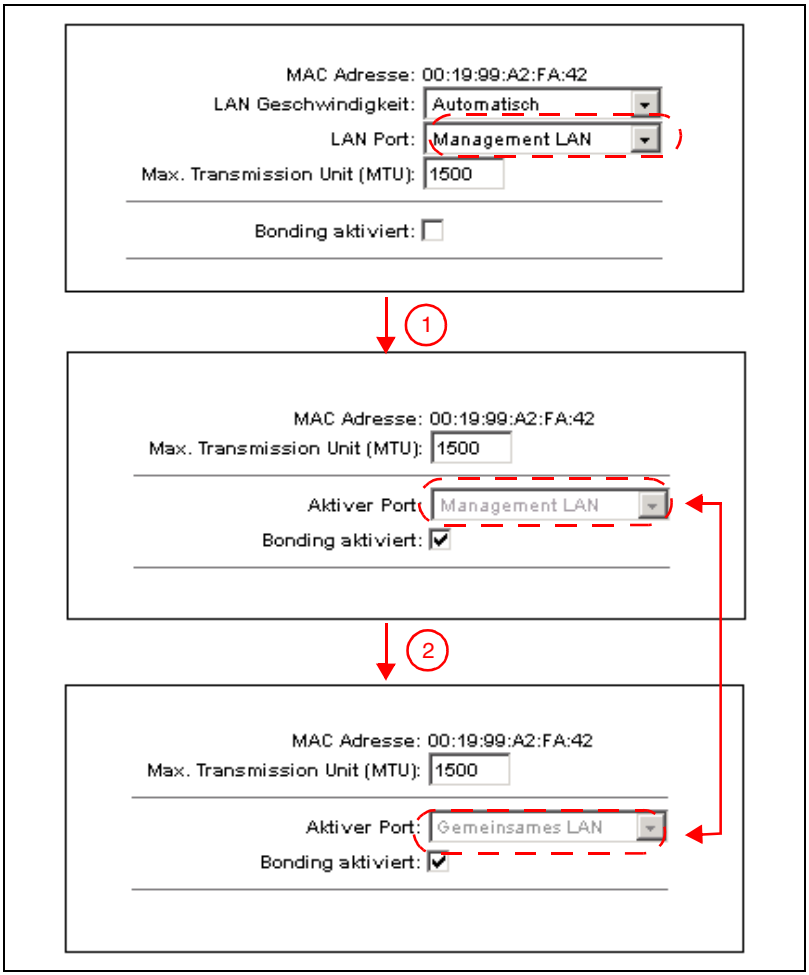



Bild 156: Aktiviertes IP-Bonding

1. Sobald das Bonding aktiviert ist, wird der derzeit verwendete LAN-Anschluss (hier: Management LAN) zum aktiven Port, der dann im Feld *Aktiver Port* angezeigt wird. Der zweite LAN-Anschluss (hier: Gemeinsames LAN) wird zum Backup-Anschluss.

2. Wenn der derzeit aktive Anschluss (hier: Management LAN) fehlschlägt („link down“), wird der sekundäre Anschluss (hier: Gemeinsames LAN) aktiv.

**Einschränkungen:**

Blade Server unterstützen keinen Netzwerk-Bonding-Modus für den iRMC S4. Sie verwenden einen automatischen Failover-Mechanismus zwischen zwei gemeinsamen LAN-Anschlüssen, um die redundante Netzwerkfunktion sicherzustellen.

*IPv4 aktiviert*

IPv4-Adressierung ist für den iRMC S4 immer aktiviert und kann nicht deaktiviert werden.

*IPv6 aktiviert*

Aktiviert/deaktiviert IPv6-Adressierung für den iRMC S4. Bei aktivierter IPv6-Adressierung wird die Gruppe *IPv6 Konfiguration* angezeigt (siehe unten).

Falls aktuell mit IPv6-Adressierung auf den iRMC S4 zugegriffen wird, können Sie die IPv6-Adressierung nicht deaktivieren.

### IPv4 Konfiguration

In der Gruppe *IPv4 Konfiguration* können Sie die IPv4-Einstellungen für den iRMC S4 konfigurieren.

*IP Address*

IPv4-Adresse des iRMC S4 im LAN. Diese Adresse unterscheidet sich von der IP-Adresse des verwalteten Servers.

Falls mit einer statischen Adresse gearbeitet wird (Option *DHCP aktiviert* nicht aktiviert), können Sie diese hier eingeben. Andernfalls (Option *DHCP aktiviert* ist aktiviert) verwendet der iRMC S4 das Feld nur zur Anzeige der Adresse.

*Subnetz Maske*

Subnetz-Maske des iRMC S4 im LAN.

*Gateway*

IP-Adresse des Default-Gateway für das LAN.

*DHCP aktiviert*

Wenn Sie diese Option aktivieren, erfragt der iRMC S4 seine LAN-Einstellungen von einem DHCP-Server im Netz.

Aktivieren Sie Option *DHCP* nicht, wenn im Netz kein DHCP-Server verfügbar ist.
Wenn Sie die Option *DHCP* aktivieren und im Netz kein DHCP-Server verfügbar ist, läuft der iRMC S4 in eine Such-Schleife (d.h. er sucht so lange nach einem DHCP-Server, bis er einen findet).

Der (konfigurierte) iRMC S4 kann von einem entsprechend konfigurierten DHCP-Server bei einem DNS-Server registriert werden (siehe Abschnitte "DNS Konfiguration - DNS für den iRMC S4 konfigurieren" auf Seite 282).

### IPv6 Konfiguration

In der Gruppe *IPv6 Konfiguration* können Sie eine IPv6-Adresse für den iRMC S4 automatisch oder manuell konfigurieren.

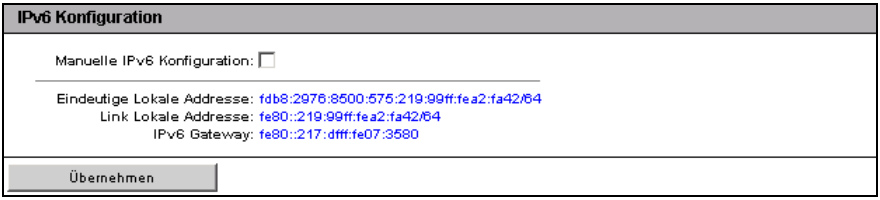



Bild 157: Seite Netzwerk Schnittstelle - Manuelle IPv6 Konfiguration deaktiviert

*Manuelle IPv6 Konfiguration*

Voreinstellung: deaktiviert

Wenn *Manuelle IPv6 Konfiguration* deaktiviert ist, wird "Stateless Autoconfiguration" oder "Stateful Address Configuration" verwendet, um automatisch eine Routing-fähige IPv6-Adresse für den iRMC S4 zu konfigurieren:

– Stateless Autoconfiguration:

  Stateless Autoconfiguration nutzt die *Link Lokale Adresse*, die dem iRMC S4 immer automatisch zugewiesen ist, und aktiviert den iRMC S4, um eine eigene IPv6-Adresse zu generieren.

– Stateful Address Configuration

  Bei Stateful Address Configuration ruft der iRMC S4 die IPv6-Adresse von einem DHCP-Server ab.

Wenn Sie die Option *Manuelle IPv6 Konfiguration* aktivieren, zeigt die *IPv6 Konfigurierung* zusätzliche Parameter an, mit der Sie manuell eine Routing-fähige IPv6-Adresse für den iRMC S4 konfigurieren können.

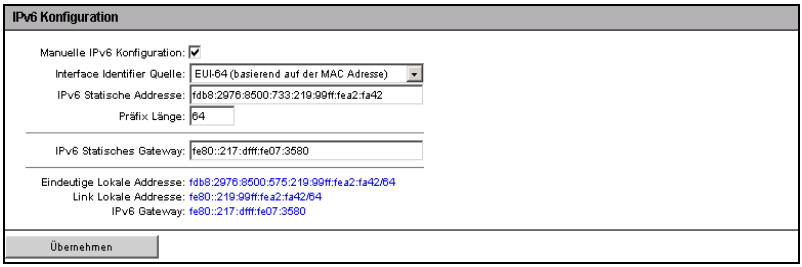



Bild 158: Seite Netzwerk Schnittstelle - Manuelle IPv6 Konfiguration

*IPv6 Statische Adresse*
: Statische IPv6-Adresse für den iRMC S4.

*Präfix Länge*
: Länge des IPv6-Präfix.

*IPv6 Statisches Gateway*
: Statische IPv6-Adresse des Default -Pv6-Gateway im LAN.

### VLAN Konfiguration

*VLAN aktiviert*
: Mithilfe dieser Option aktivieren Sie die VLAN-Unterstützung für den iRMC S4.

*VLAN Id*
: VLAN-Identifier des virtuellen Netzes (VLAN), dem der iRMC S4 angehört. Zulässiger Bereich: 1 $\leq$ *VLAN Id* $\leq$ 4094.

*VLAN Priorität*
: VLAN-Priorität (Benutzerpriorität) des iRMC S4 in dem durch *VLAN Id* spezifizierten VLAN.
Zulässiger Bereich: 0 $\leq$ *VLAN Priority* $\leq$ 7 (default: 0).

## 7.13.2 Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren

Mit der Seite *Ports und Netzwerk Dienste* können Sie die Konfigurationseinstellungen für die Ports und Netzwerk-Dienste einsehen und ändern.

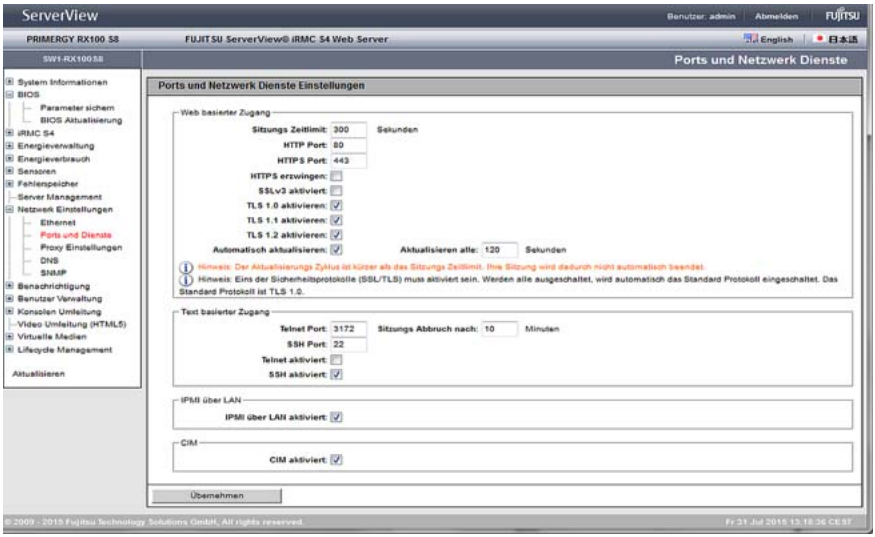



Bild 159: Seite Ports und Netzwerk Dienste

Für Ports, deren Eingabefelder an der iRMC S4-Weboberfläche deaktiviert sind, wird eine Konfiguration nicht unterstützt.

### Ports für Web-basierten Zugang

*Sitzungs Zeitlimit*

Zeitspanne (in Sekunden), nach deren Verstreichen Ihre Sitzung bei Inaktivität automatisch beendet wird. Es wird dann die Anmelde-Seite der iRMC S4-Weboberfläche angezeigt, über die Sie sich erneut anmelden können (siehe Seite 134).

Ihre Sitzung wird nicht automatisch beendet, wenn sie inaktiv ist und die unter *Sitzungs Zeitlimit* festgelegte Zeit abgelaufen ist und Sie einen Wert für das Aktualisierungsintervall eingeben, der unter dem Wert für *Sitzungs Zeitlimit* im Feld *Aktualisieren alle ... Sekunden* liegt.

*HTTP Port*

HTTP Port des iRMC S4
Standard-Portnummer: 80
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend und ausgehend

*HTTPS Port*

HTTPS (HTTP Secure) Port des iRMC S4
Standard-Portnummer: 443
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend und ausgehend

*HTTPS erzwingen*

Wenn Sie *HTTPS erzwingen* aktivieren, können die Benutzer nur über den im Eingabefeld angegebenen HTTPS-Port eine gesicherte Verbindung zum iRMC S4 aufbauen.

Wenn Sie *HTTPS erzwingen* deaktivieren, können die Benutzer über den im Eingabefeld angegebenen HTTP Port eine nicht-gesicherte Verbindung zum iRMC S4 aufbauen.

Wenn das SSL-Zertifikat ausgelaufen ist, wird am Browser eine entsprechende Meldung ausgegeben.

*SSLv3 aktiviert*

Erlaubt eine HTTPS-Sitzung mit SSL V3.

*TLS 1.0 aktivieren*

Erlaubt eine HTTPS-Sitzung mit TLS V1.0.

*TLS 1.1 aktivieren*
Erlaubt eine HTTPS-Sitzung mit TLS V1.1.

*TLS 1.2 aktivieren*
Erlaubt eine HTTPS-Sitzung mit TLS V1.2.

*Automatisch aktualisieren*
Wenn Sie diese Option aktivieren, wird die Anzeige der iRMC S4-Weboberfläche automatisch periodisch aktualisiert. Das Aktualisierungsintervall spezifizieren Sie im Eingabefeld *Aktualisieren alle ... Sekunden*.

*Aktualisieren alle ... Sekunden*
Länge (in Sekunden) des Intervalls für die automatische Aktualisierung der iRMC S4-Weboberfläche.

Wenn Sie das Aktualisierungsintervall kleiner wählen als den Wert für das *Sitzungs Zeitlimit* (siehe Seite 277), wird Ihre Sitzung auch bei Inaktivität nicht automatisch nach Ablauf der bei *Sitzungs Zeitlimit* spezifizierten Zeit beendet.

### Ports für Text-basierten Zugang

*Telnet Port*
Telnet Port des iRMC S4
Standard-Portnummer: 3172
Konfigurierbar: ja
Standardmäßig aktiviert: nein
Kommunikationsrichtung: eingehend und ausgehend

*Sitzungs Abbruch nach ... Sekunden*
Zeitspanne (in Minuten), nach deren Verstreichen eine Telnet / SSH-Verbindung bei Inaktivität automatisch abgebaut wird.

*SSH Port*
SSH (Secure Shell) Port des iRMC S4
Standard-Portnummer: 22
Konfigurierbar: ja
Standardmäßig aktiviert: ja
Kommunikationsrichtung: eingehend und ausgehend

*Telnet aktiviert*
Wenn Sie *Telnet aktiviert* aktivieren, können die Benutzer über den im Eingabefeld Telnet Port angegebenen Port eine Verbindung zum iRMC S4 aufbauen.

*SSH aktiviert*

Wenn Sie *Telnet aktiviert* aktivieren, können die Benutzer über den im Eingabefeld Telnet Port angegebenen Port eine Verbindung zum iRMC S4 aufbauen.

### IPMI over LAN

"IPMI-over-LAN" ist die Spezifikation der LAN-Schnittstelle im IPMI-Standard. Diese Spezifikation legt fest, wie IPMI-Mitteilungen an den bzw. vom iRMC gesendet werden können – verkapselt in RMCP (Remote Management Control Protocol)-Datenpakete. Diese RMCP-Datenpakete werden über eine Ethernet LAN-Verbindung mit UDP unter IPv4 oder IPv6 übertragen.

RCMP unterstützt das Management von Systemstatus in Systemen ohne laufendes Betriebssystem.

Die Schnittstelle für eine solche Verbindung wird auf dem integrierten LAN-Controller des iRMC bereitgestellt.

*IPMI über LAN aktiviert*

Diese Option ist standardmäßig aktiviert.
Dies ermöglicht es Ihnen, die Funktion "IPMI over LAN" zu deaktivieren.

### CIM

Das Common Information Model (CIM) ist ein standardisiertes, hierarchisches, objektorientiertes Datenmodell, das eine einheitliche Darstellung von verwalteten Ressourcen sicherstellt.

*CIM aktiviert*

Diese Option ist standardmäßig aktiviert.
Erlaubt Ihnen, das CIM-Protokoll zu deaktivieren.

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre konfigurierten Einstellungen zu speichern.

## 7.13.3 Proxy Einstellungen– Proxyeinstellungen konfigurieren

Auf der Seite *Proxy Einstellungen* können Sie die Einstellungen für einen Proxyserver konfigurieren, der optional für die Herstellung einer Verbindung zu einem Update-Repository (siehe Abschnitt "Aktualisierungs Einstellungen – allgemeine eLCM-Update-Einstellungen konfigurieren" auf Seite 365) und/oder für die Herstellung einer AIS Connect-Verbindung (siehe Abschnitt "AIS Connect – AIS Connect konfigurieren und verwenden" auf Seite 157) verwendet werden kann.

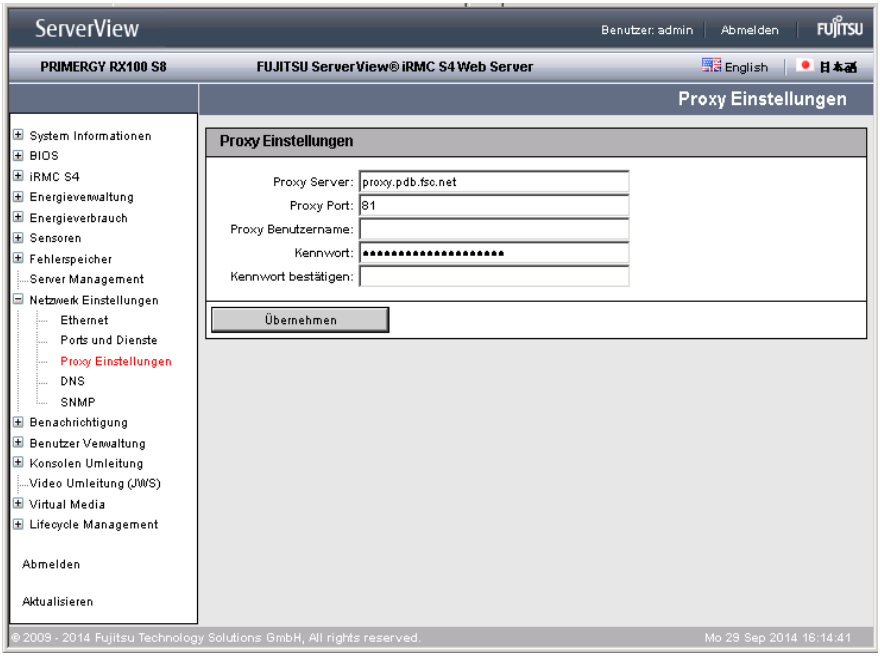



Bild 160: Seite "Proxy Einstellungen"

*Proxy Server*

IP-Adresse des Proxy-Servers

Sie können für den iRMC S4 den Domain Name System (DNS) aktivieren (siehe "DNS Konfiguration - DNS für den iRMC S4 konfigurieren" auf Seite 282). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

*Proxy Port*

Anschluss des Proxy-Service.
Standard-Portnummer: 81

*Proxy Benutzername*

Benutzername für die Authentisierung beim Proxy-Server

*Kennwort*

Kennwort für die Authentisierung beim Proxy-Server

*Kennwort bestätigen*

Bestätigen Sie hier Ihr Kennwort.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

## 7.13.4 DNS Konfiguration - DNS für den iRMC S4 konfigurieren

Mit der Seite *DNS Konfiguration* können Sie für den iRMC S4 den Domain Name System (DNS) aktivieren und einen Hostnamen für den iRMC S4 konfigurieren.

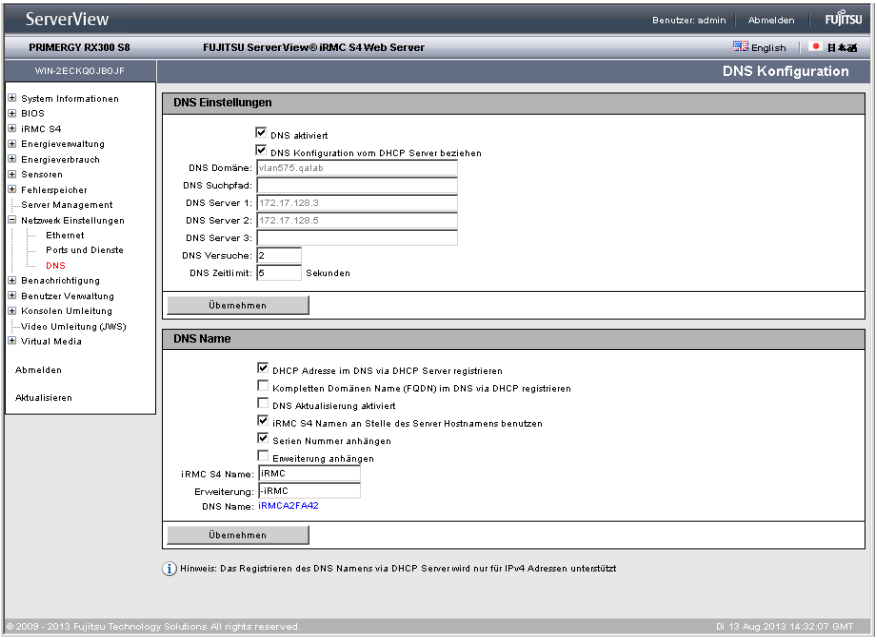



Bild 161: Seite DNS Konfiguration

### DNS Einstellungen

Die Gruppe *DNS Einstellungen* ermöglicht Ihnen die Aktivierung des Domain Name System (DNS) für den iRMC S4. Dadurch können Sie symbolische DNS-Namen anstelle von IP-Adressen verwenden, um den iRMC S4 zu konfigurieren.

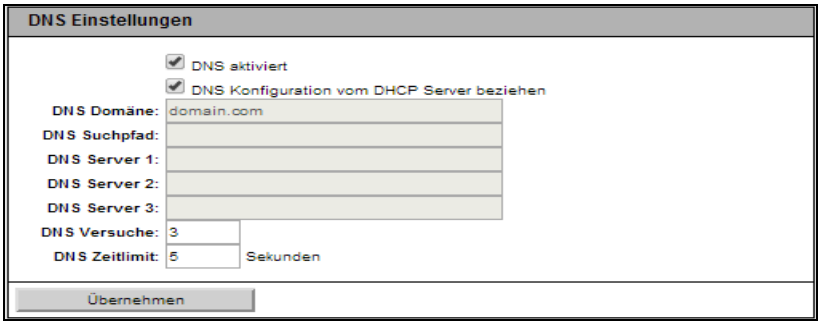



Bild 162: Seite DNS Konfiguration - DNS Einstellungen

*DNS aktiviert*

Aktiviert / deaktiviert DNS für den iRMC S4.

*DNS Konfiguration vom DHCP Server beziehen*

Wenn Sie diese Option aktivieren, werden die IP-Adressen der DNS-Server automatisch vom DHCP-Server übernommen.
In diesem Fall werden bis zu drei DNS-Server unterstützt.

Wenn Sie diese Einstellung nicht aktivieren, können Sie unter *DNS-Server 1* - *DNS-Server 3* bis zu drei DNS-Serveradressen manuell eingeben.

*DNS Domäne*

Wenn die Option *DNS Konfiguration vom DHCP Server beziehen* deaktiviert ist, geben Sie hier den Namen der Default-Domäne für Anfragen an den bzw. die DNS Server an.

*DNS Suchpfad*

Liste der (teilweise qualifizierten) Domänennamen, getrennt durch eine oder mehrere Leerzeichen. Die DNS-Suchliste kann maximal 256 Zeichen enthalten. Das Feld „DNS Suchpfad“ wird verwendet, um die Domänen festzulegen, die durchsucht werden, wenn Sie einen Hostnamen suchen, der über keine Domänenname-Komponente verfügt.

*DNS Server 1 .. 3*

Wenn die Option *DNS Konfiguration vom DHCP Server beziehen* eaktiviert ist, können Sie hier die IP-Adressen von bis zu fünf der DNS-Servern angeben.

*DNS Versuche*

Anzahl der DNS-Retries.

*DNS Zeitlimit*

Zeitlimit (in Sekunden) für eine Antwort des DNS.

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre konfigurierten Einstellungen zu speichern.

### DNS Name

In der Gruppe *DNS Name* können Sie einen Hostnamen für den iRMC S4 konfigurieren und so „dynamic DNS“ nutzen. Mit „Dynamic DNS“ können DHCP-Server die IP-Adresse und den Systemname einer Netzkomponente selbstständig zur besseren Identifikation an DNS-Server weitergeben.

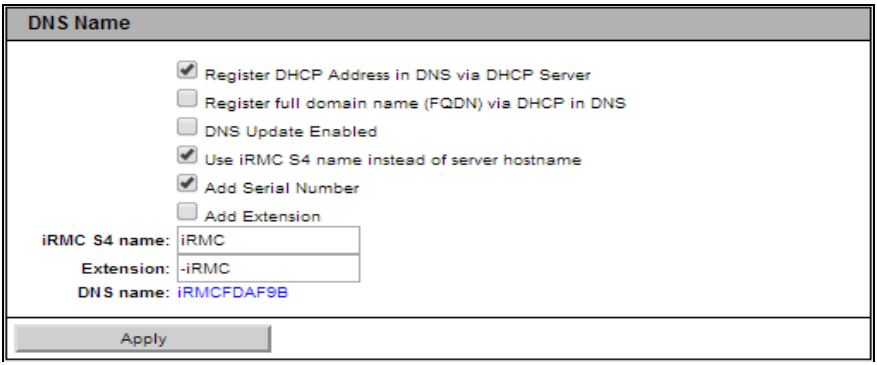

DNS Name
Register DHCP Address in DNS via DHCP Server
Register full domain name (FQDN) via DHCP in DNS
DNS Update Enabled
Use iRMC S4 name instead of server hostname
Add Serial Number
Add Extension
iRMC S4 name: iRMC
Extension: -iRMC
DNS name: iRMCFDAF9B
Apply

Bild 163: Seite DNS Konfiguration - DNS Name

*DHCP Adresse im DNS via DHCP Server registrieren*

Wenn IPv6-Adressierung verwendet wird, ist diese Option deaktiviert. Aktiviert / deaktiviert für den iRMC S4 die DHCP-Namensübergabe an den DHCP Server sowie die DNS Registrierung via DHCP Server.

*Kompletten Domain Name (FQDN) im DNS via DHCP Server registrieren*

Wenn IPv6-Adressierung verwendet wird, ist diese Option deaktiviert. Aktiviert / deaktiviert für den iRMC S4 die Übergabe des FQDN (Fully Qualified Domain Name) an den DHCP Server sowie die DNS Registrierung via DHCP Server.

*DNS Aktualisierung aktiviert*

Aktiviert / deaktiviert die Aktualisierung von DNS Records via Dynamic DNS.

Nur unsicherer DNS wird unterstützt.

*iRMC S4 Namen an Stelle des Server Hostnamens benutzen*

Der im Dialogfeld *iRMC S4 Name* spezifizierte iRMC S4-Name wird anstelle des Servernamens verwendet.

*Serien Nummer anhängen*

Dem DHCP-Namen für den iRMC S4 werden rechts die letzten 3 Bytes der MAC-Adresse des iRMCS4 hinzugefügt.

*Erweiterung anhängen*

Dem DHCP-Namen für den iRMC S4 wird die im Dialogfeld *Erweiterung* eingetragene Erweiterung hinzugefügt.

*iRMC S4 Name*

iRMC S4-Name, der für den iRMC S4 anstelle des Servernamens an DHCP weitergegeben wird. Abhängig von den entsprechenden Optionen wird der iRMC S4-Name als Bestandteil des DNS-Namens verwendet.

*Erweiterung*

Namenserweiterung für den iRMC S4.

*DNS Name*

Zeigt den konfigurierten DNS-Namen für den iRMC S4.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre konfigurierten Einstellungen zu speichern.

## 7.13.5 SNMP Allgemeine Konfiguration

Auf der Seite *SNMP Allgemeine Konfiguration* können Sie auf dem iRMC S4 einen SNMP-Dienst konfigurieren, der SNMP v1/v2c und SNMPv3 GET-Anforderungen auf den folgenden SNMP MIBs unterstützt:

– SNMP MIB-2

– SNMP STATUS.MIB

– SNMP OS.MIB

– SNMP SC2.MIB

– SNMP RAID.MIB

Wenn der SNMP-Dienst aktiviert ist, können die von diesen MIBs bereitgestellten Informationen von jedem System verwendet werden, auf dem ein SNMP-Manager ausgeführt wird.

SNMPv3 stellt eine höhere Sicherheitsstufe als SNMPv1 oder SNMPv2c bereit.

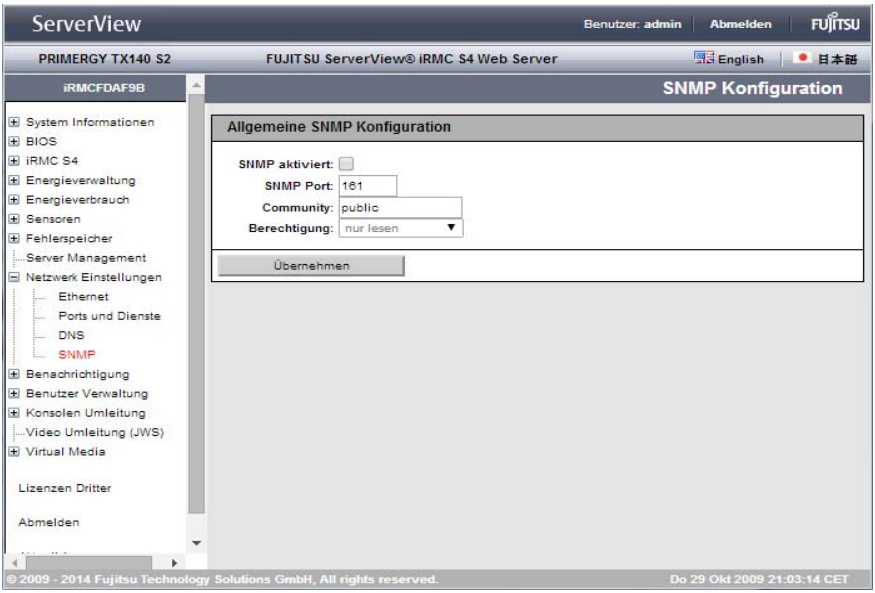


Bild 164: Seite "SNMP Konfiguration"

*SNMP aktiviert*

Aktiviert den SNMP-Dienst auf dem iRMC S4.

*SNMP Port*

Port, an den der SNMP-Dienst die SNMP lauscht (normalerweise UDP 161). Sie können für jeden Benutzer konfigurieren, ob er SNMP verwenden darf, siehe Abschnitt "Benutzer Verwaltung - lokale Benutzerverwaltung am iRMC S4".

*SNMP-Protokoll*

Zu verwendende Version des SNMP-Protokolls.

*Alle (SNMPv1/v2c/v3)*

Der SNMP-Dienst ist für alle Versionen des SNMP-Protokolls (SNMP v1/v2c/v3) verfügbar.

*Nur SNMPv3*

Nur SNMPv3 ist verfügbar.

Die folgenden beiden Optionen werden nur angezeigt, wenn unter *SNMP-Protokoll* die Option *Alle (SNMPv1/v2c/v3)* ausgewählt wurde.

*SNMPv1/v2c Community*

Community-String im Fall von SNMP v1/v2c.

Der Communicty-String darf folgende Zeichen enthalten:

A-Z,a-z,0-9(*/:,_?=-@&)%!

Leerzeichen und \ sind nicht erlaubt.

Im SNMP-Sprachgebrauch ist eine "Community" eine Gruppe aus mindestens einer Management-Plattform. Jede Community wird durch eine Community-Zeichenfolge gekennzeichnet. Bei der Community-Zeichenfolge handelt es sich um eine unverschlüsselte Komponente jedes SNMP-Requests, die den Sender des Requests als Mitglied der jeweiligen Community identifiziert. Daher wird die Autorisierung für einen SNMP GET-Request durch diese Community-Zeichenfolge gesteuert. Die Community-Zeichenfolge stellt einen einfachen Authentifizierungsmechanismus in SNMP zur Verfügung.

Da die Community-Zeichenfolge unverschlüsselt mit der SNMP-Nachricht gesendet wird, besteht jederzeit das Risiko, das sie unberechtigt verwendet wird. Dies kann im Hinblick auf die Sicherheit beim Einsatz von SNMP zum Problem werden. Andererseits verwenden die meisten Communitys auf jeden Fall die vorgegebene Community-Zeichenfolge "public".

*SNMPv1/v2c Berechtigung*

Berechtigung für die SNMP Community. Derzeit wird "nur lesen" unterstützt (fester vorgegebener Wert).

- Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre konfigurierten Einstellungen zu speichern.

# 7.14 Benachrichtigungen - Alarmbenachrichtigung konfigurieren

Der Eintrag *Benachrichtigungen* enthält die Verweise auf die Seiten, mit denen Sie die Alarmbenachrichtigung (Alerting) für den iRMC konfigurieren können:

– "SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren" auf Seite 290.

– "E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren" auf Seite 292.

## 7.14.1 SNMP Trap Benachrichtigung - SNMP Trap-Benachrichtigung konfigurieren

In der Seite *SNMP Trap Benachrichtigung* können Sie die Einstellungen der SNMP Trap-Benachrichtigung (SNMP-Alarmweiterleitung) einsehen und konfigurieren.

Traps werden unabhängig davon gesendet, ob SNMP aktiviert ist oder nicht. Sie werden über die net-snmp-Schnittstelle gesendet, um SNMPv1 / V2c und SNMPv3-Traps zu unterstützen.

Es wird die Weiterleitung von SNMP-Traps an bis zu sieben SNMP-Server unterstützt.

Sie können für jeden Benutzer konfigurieren, ob er SNMP verwenden darf, siehe Kapitel "iRMC-Weboberfläche" auf Seite 299.

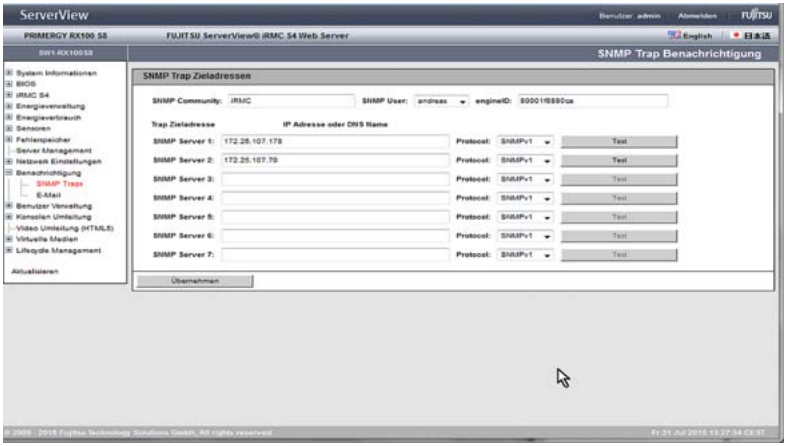


Bild 165: Seite SNMP Trap Benachrichtigung

*SNMP Community*
Name der SNMP-Community.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um den Community-Namen zu übernehmen.

*SNMP User*
Vorkonfigurierter SNMPv3-Benutzer für SNMPv3-Trap-Ziel.

*engineID*

wird verwendet, um SNMPv3-Traps zu senden. Die ID kann gemäß RFC3411 geändert werden. Die ID muss innerhalb des Sets der kommunizierenden SNMPv3-Agenten und Manager einzigartig sein. Die Regeln für eine *engineID* sind wie folgt:

- Die ID-Länge muss mindestens fünf Oktette, aber höchstens 32 Oktette betragen. Jedes Oktett kann einen Wert zwischen 0 und 255 enthalten (hexadezimal: 0x00 bis 0xff).
- Eine SNMP-*engineID* darf nicht nur aus Oktetten mit dem Wert 0 oder 255 bestehen (hexadezimal: 0xff).
- Wenn eine *engineID* mit einer 0 anfängt, muss sie mindestens 12 Oktette lang sein.
- Für jede *engineID* muss ein Eintrag *createUser* in der Konfiguration für den SNMP-Trap-Empfänger vorliegen.

*SNMP Server1 .. SNMP Server7* (Trap-Ziele)

DNS-Namen oder IP-Adressen der Server, die dieser SNMP-Community angehören und als *Trap-Ziele* konfiguriert werden sollen.

- ► Klicken Sie auf die Schaltfläche *Übernehmen*, um den SNMP Server als Trap-Ziel zu aktivieren.
- ► Klicken Sie auf die Schaltfläche *Test*, um die Verbindung zum SNMP Server zu testen.

► Klicken Sie gegebenenfalls auf die Schaltfläche *Alle übernehmen*, um alle Einstellungen zu aktivieren.

## 7.14.2 E-Mail Benachrichtigung- Lokale E-Mail-Benachrichtigung konfigurieren

Mithilfe der Seite *Mail Benachrichtigung* konfigurieren Sie die Einstellungen für die E-Mail-Benachrichtigung an lokale Benutzerkennungen.
E-Mail-Benachrichtigung an lokale Benutzerkennungen.

Es wird die Konfiguration von zwei Mail Servern unterstützt.

E-Mail-Benachrichtigung kann für jeden Benutzer individuell festgelegt werden (siehe Abschnitt "Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)" auf Seite 302).

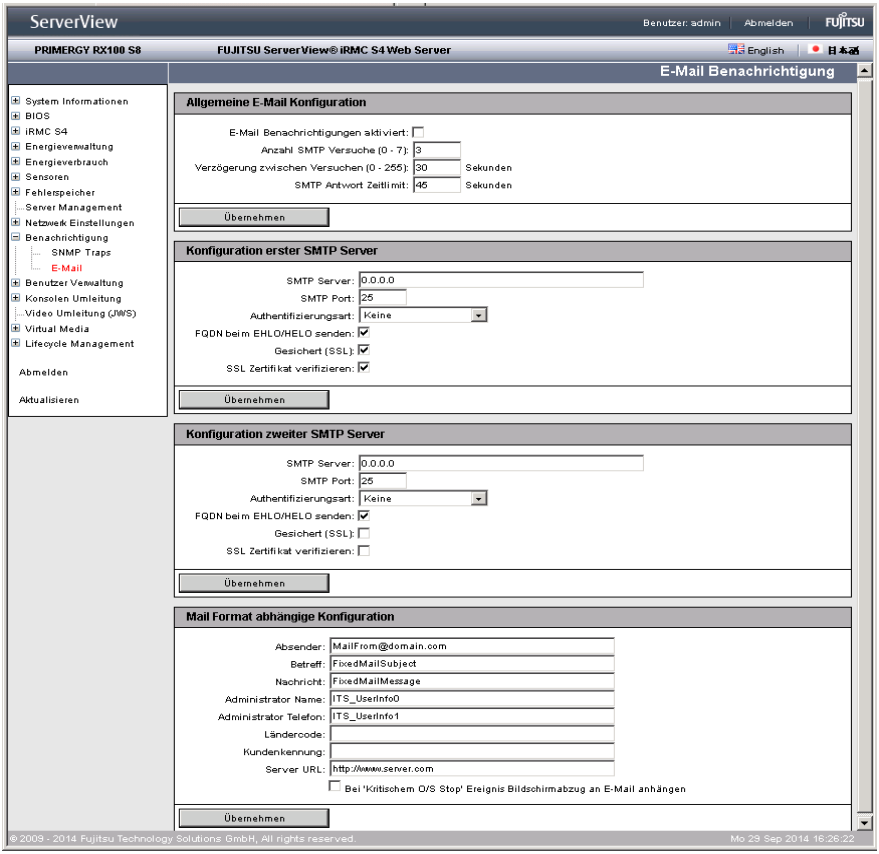



Bild 166: Seite E-Mail Benachrichtigung

### Allgemeine E-Mail Konfiguration - Allgemeine E-Mail-Einstellungen konfigurieren

Mit der Gruppe *Allgemeine E-Mail Konfiguration* konfigurieren Sie die allgemeinen E-Mail-Einstellungen.

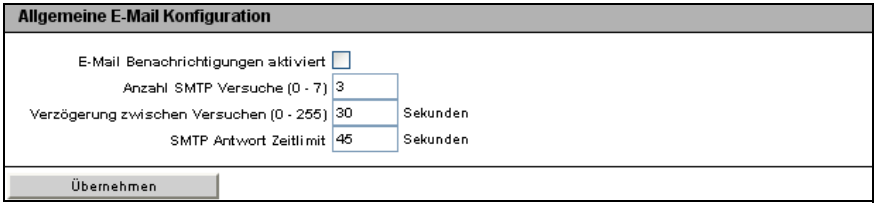



Bild 167: Seite E-Mail Benachrichtigung - Allgemeine E-Mail Konfiguration

*Mail Benachrichtigungen aktiviert*
Aktivieren Sie diese Option.

*SMTP Anzahl Versuche (0 - 7)*
Anzahl möglicher SMTP-Versuche.

*Verzögerungen zwischen Versuchen (0 - 255)*
Zeitspanne (in Sekunden) zwischen den einzelnen SMTP-Versuchen.

*SMTP Antwort Zeitlimit*
Zeitlimit (in Sekunden) für SMTP-Antwort.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Konfiguration erster SMTP Server - Ersten Mail Server konfigurieren

Mit der Gruppe *Konfiguration erster SMTP Server* konfigurieren Sie den ersten (primären) Mail Server (SMTP Server).

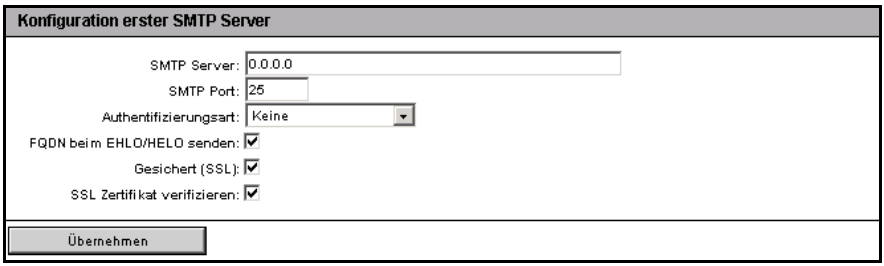



Bild 168: Seite E-Mail Benachrichtigung - Konfiguration erster SMTP Server

*SMTP Server*

IP-Adresse des primären Mail Servers.

Sie können für den iRMC S4 den Domain Name System (DNS) aktivieren (siehe "DNS Konfiguration - DNS für den iRMC S4 konfigurieren" auf Seite 282). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

*SMTP Port*

SMTP Port des Mail Servers

*Authentifizierungs Art*

Art der Authentifizierung einer Verbindung des iRMC S4 zum Mail Server:

– *Keine*
Keinerlei Authentifizierung der Verbindung.

– *SMTP AUTH (RFC 2554)*
Authentifizierung gemäß RFC 2554: SMTP-Service-Erweiterung für Authentifizierung.

In diesem Fall werden folgende Eingaben erwartet:

*Auth. Benutzer Name*
Benutzername für die Authentisierung beim Mail Server

*Auth. Kennwort*
Kennwort für die Authentisierung beim Mail Server

*Kennwort bestätigen*
Bestätigen Sie hier Ihr Kennwort.

*FQDN beim EHLO/HELO senden*

Aktiviert/deaktiviert den Versand des FDQN mit EHLO/HELO.

*Secure (SSL)*

Abhängig vom konfigurierten Netzwerkanschluss stellt der iRMC S4 direkt eine SSL-Verbindung her (SMTPS-Legacy-Anschluss 465) oder prüft, ob das Schlüsselwort `STARTTLS` enthalten ist (jeder andere konfigurierte Netzwerkanschluss):

– Wenn `STARTTLS` in der Antwort vom SMTP-Server enthalten ist, wechselt der iRMC S4 auf der bestehenden Netzwerkverbindung zu TLS.

– Wenn `STARTTLS` nicht enthalten ist, wird die Nachricht unverschlüsselt über die bestehende Verbindung gesendet.

E-Mails werden SSL-verschlüsselt gesendet.

*SSL Zertifikat verifizieren*
Das SSL-Zertifikat vom SMTP-Server wird anhand des gespeicherten Zertifizierungsstellenzertifikats im iRMC S4 verifiziert (z. B. muss das SMTP-Server-Zertifikat von dieser Zertifizierungsstelle ausgestellt/unterzeichnet sein).

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Konfiguration zweiter SMTP Server - Zweiten Mail Server konfigurieren

Mit der Gruppe *Konfiguration zweiter SMTP Server* konfigurieren Sie den zweiten (sekundären) Mail Server (SMTP Server).

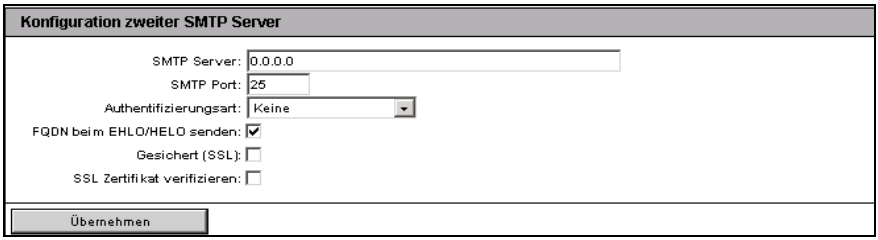



Bild 169: Seite E-Mail Benachrichtigung - Konfiguration zweiter SMTP Server

*SMTP Server*
IP-Adresse des sekundären Mail Servers.

Sie können für den iRMC S4 den Domain Name System (DNS) aktivieren (siehe "DNS Konfiguration - DNS für den iRMC S4 konfigurieren" auf Seite 282). Anstelle der IP-Adresse können Sie dann einen symbolischen Namen angeben.

*SMTP Port*
SMTP Port des Mail Servers

*Authentifizierungs Art*
Art der Authentifizierung einer Verbindung des iRMC S4 zum Mail Server:

– *Keine*
Keinerlei Authentifizierung der Verbindung.

– *SMTP AUTH (RFC 2554)*
Authentifizierung gemäß RFC 2554: SMTP-Service-Erweiterung für Authentifizierung.

In diesem Fall werden folgende Eingaben erwartet:

*Auth. Benutzer Name*
Benutzername für die Authentisierung beim Mail Server

*Auth. Kennwort*
Kennwort für die Authentisierung beim Mail Server

*Kennwort bestätigen*
Bestätigen Sie hier Ihr Kennwort.

*FQDN beim EHLO/HELO senden*
Aktiviert/deaktiviert den Versand des FDQN mit EHLO/HELO.

*Secure (SSL)*
E-Mails werden SSL-verschlüsselt gesendet.

*SSL Zertifikat verifizieren*
Das SSL-Zertifikat wird verifiziert.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Mail Format abhängige Konfiguration - Mail-Format-abhängige Einstellungen konfigurieren

Mit der Gruppe *Mail Format abhängige Konfiguration* konfigurieren Sie die vom Mail-Format abhängigen Einstellungen. Das Mail-Format konfigurieren Sie Benutzer-spezifisch auf der Seite *Neuen Benutzer konfigurieren* - *Benutzer '<Name>' Konfiguration* - *E-Mail Konfiguration* (siehe Seite 310).

Es werden die folgenden Mail-Formate unterstützt:

– Standard
– Fixed Subject
– ITS-Format
– SMS-Format

Bild 170: Seite E-Mail Benachrichtigung - Mail Format abhängige Konfiguration

Je nach Mail-Format sind nicht alle Eingabefelder aktiv.

*Absender*

Absenderidentifizierung für iRMC S4.
Aktiv bei allen Mail-Formaten.

Wenn in der hier eingegebenen Zeichenfolge ein „@“ enthalten ist, wird diese Zeichenfolge als gültige E-Mail-Adresse interpretiert. Andernfalls wird „admin@<ip-adresse>“ als gültige E-Mail-Adresse verwendet.

*Betreff*

Betreff der Alarmmeldung-E-Mails.
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 310).

*Nachricht*

Art der Mitteilung (E-Mail)
Aktiv nur bei Mail-Format *Fixed Subject* (siehe Seite 310).

*Administrator Name*

Name des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 310).

*Administrator Telefon*

Telefonnummer des verantwortlichen Administrators (optional).
Aktiv nur bei Mail-Format *ITS* (siehe Seite 310).

*Ländercode*

Zweistelliger Ländercode basierend auf ISO 3166 Alpha 2.

*Kundenkennung*

Kennung des Kunden.

*Server URL*

Eine URL, unter der der Server unter bestimmten Voraussetzungen zugänglich ist. Sie müssen die URL manuell eingeben.
Aktiv nur bei Mail-Format *Standard*.

*Bei 'Kritischem O/S Stop' Ereignis Bildschirmabzug an E-Mail anhängen*

Ein Screenshot, der im Falle eines kritischen Betriebssystemstopps automatisch vom iRMC S4 erstellt wird, wird an die entsprechende E-Mail für das Ereignis "kritischer Betriebssystemstopp" angehängt.

Die Erstellung des Screenshots kann aus verschiedenen Gründen fehlschlagen (z. B. nicht unterstützter Grafikmodus). Wenn deshalb nicht innerhalb von 45 Sekunden ein Screenshot zur Verfügung steht, wird die E-Mail ohne Anhang gesendet.

► Klicken Sie auf die Schaltfläche *Übernehmen*, um Ihre Einstellungen zu speichern.

# 7.15 Benutzerverwaltung

Der Eintrag *Benutzerverwaltung* enthält die Verweise auf die Seiten für die lokale Benutzerverwaltung sowie für die Konfiguration des Verzeichnisdienstes (Directory Service) zur globalen Benutzerverwaltung (LDAP-Konfiguration):

– "Benutzer Verwaltung - lokale Benutzerverwaltung am iRMC S4" auf Seite 299.

– "Verzeichnisdienst Konfiguration (LDAP) - Verzeichnisdienst am iRMC S4 konfigurieren" auf Seite 313.

– "Centralized Authentication Service (CAS) Konfiguration - CAS Konfiguration" auf Seite 335.

## 7.15.1 Benutzer Verwaltung - lokale Benutzerverwaltung am iRMC S4

Die Seite *iRMC S4 Benutzer* enthält eine tabellarische Übersicht über alle konfigurierten Benutzer: Pro Zeile werden die Daten eines konfigurierten Benutzers dargestellt. Die Benutzernamen sind dabei als Verweise realisiert. Durch Klicken auf einen Benutzernamen öffnet sich das Fenster *Benutzer '<name>' Konfiguration* (siehe Seite 302), in dem Sie die Einstellungen des betreffenden Benutzers einsehen und/oder modifizieren können.

Die Benutzer Id 1 („Null-User“) ist reserviert für den Standard und steht deshalb nicht für die Benutzerverwaltung am iRMC S4 zur Verfügung.

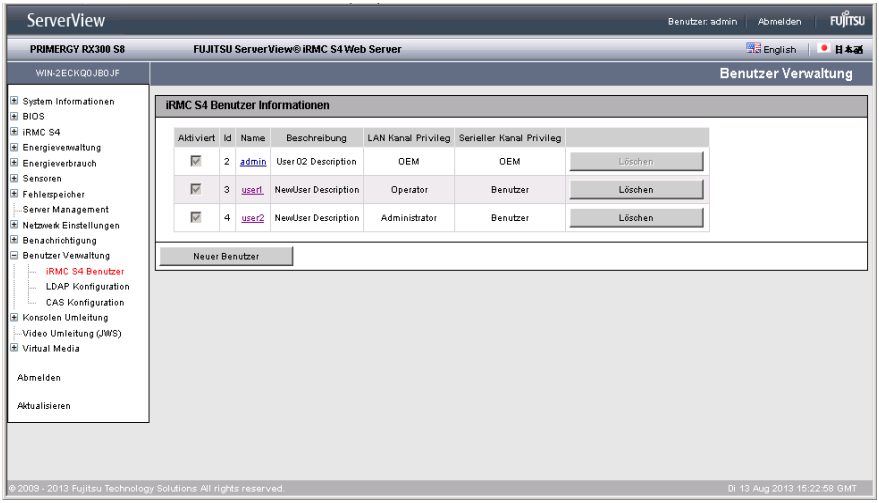



Bild 171: Seite Benutzer Verwaltung

*Löschen*

In der Tabelle der konfigurierten Benutzer finden Sie hinter jedem Benutzereintrag eine Schaltfläche *Löschen*. Durch Klicken auf diese Schaltfläche können Sie den zugehörigen Benutzer nach nochmaliger Bestätigung löschen.

*Neuer Benutzer*

Wenn Sie auf diese Schaltfläche klicken, öffnet sich die Seite *Neuen Benutzer konfigurieren* (siehe Seite 301). Hier können Sie einen neuen Benutzer konfigurieren.

### 7.15.1.1 Neuen Benutzer konfigurieren

Mithilfe der Seite *Neuen Benutzer konfigurieren* konfigurieren Sie die Grundeinstellungen eines neuen Benutzers.

Erläuterungen zu den Feldern und Auswahllisten der Seite *Neuen Benutzer konfigurieren* finden Sie ab Seite 303 bei der Beschreibung der Seite *Benutzer '<Name>' Konfiguration*.

In Bild 172 ist die Konfiguration eines Benutzers „user3“ dargestellt.

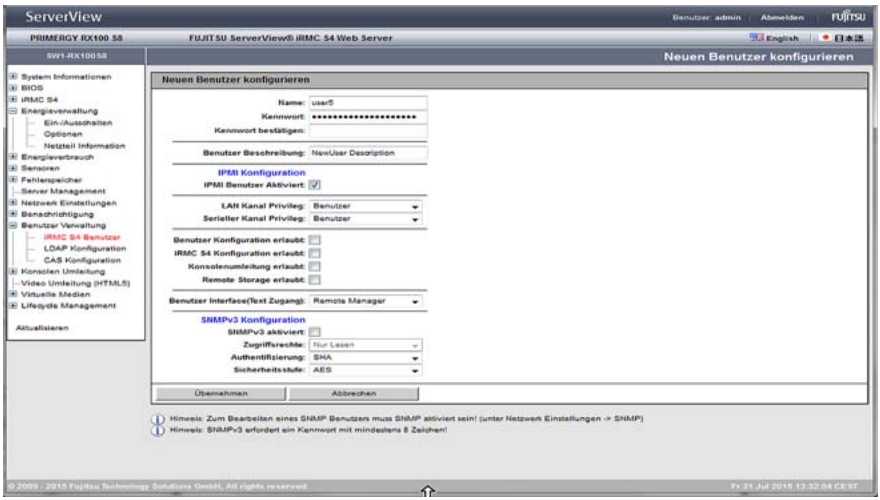


Bild 172: Seite Benutzer Verwaltung - Neuen Benutzer konfigurieren

### 7.15.1.2 Benutzer '<name>' Konfiguration - Benutzerkonfiguration (Details)

Mithilfe der Seite *Benutzer '<name>' Konfiguration* können Sie die Einstellungen für einen Benutzer einsehen, ändern und erweitern.

In Bild 173 ist die Konfiguration des in Bild 172 neu angelegten Benutzers user3 dargestellt.

Die Benutzer Id wird, in Klammern eingeschlossen, hinter dem Benutzernamen angezeigt.

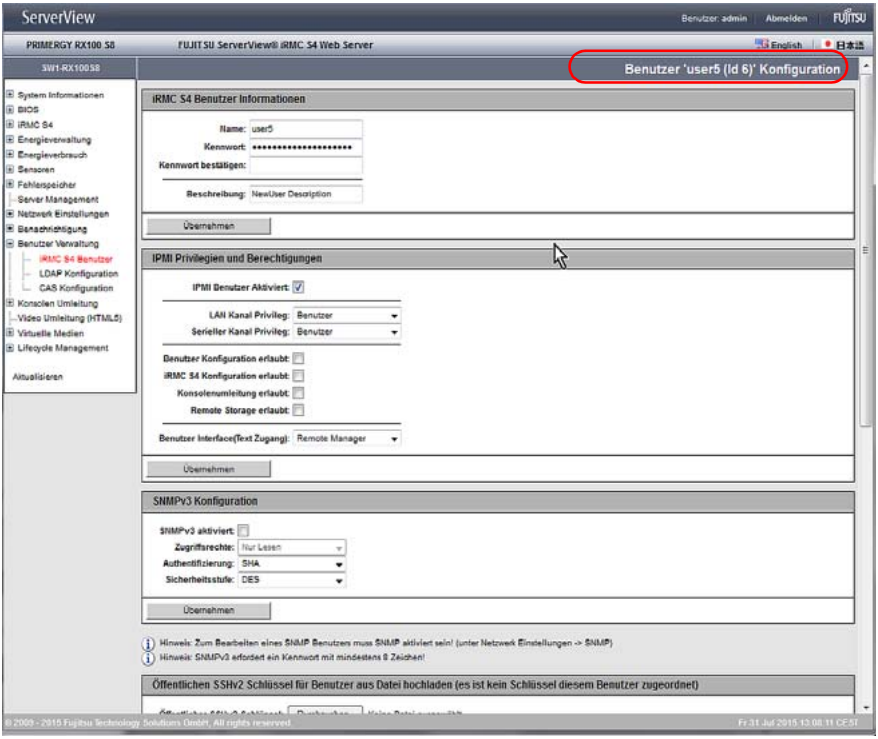


Bild 173: Benutzer Verwaltung - Benutzer "<Name>"

### Benutzer Informationen - Zugangsdaten des Benutzers konfigurieren

Mit der Gruppe *Benutzer Informationen* konfigurieren Sie die Zugangsdaten des Benutzers.

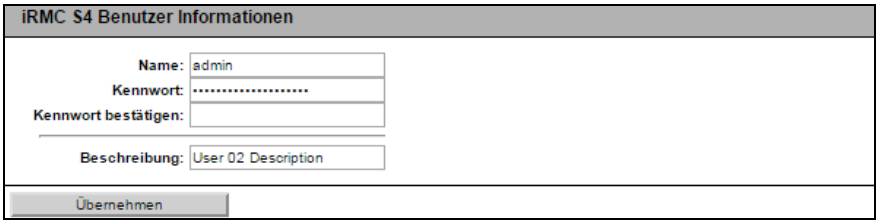



Bild 174: Benutzer '<name>' Konfiguration - iRMC S2/S3 Benutzer Informationen

*Name*

Tragen Sie hier den Namen des Benutzers ein.

Ein gültiger Benutzername muss mit einem Buchstaben beginnen. Der verbleibende Teil des Namens darf nur Buchstaben, Zahlen, Unterstriche, Bindestriche, Punkte und das @-Symbol enthalten. Leerzeichen sind nicht zulässig.

Benutzernamen müssen eindeutig sein. Duplizierte Benutzernamen sind nicht zulässig.

*Kennwort*

Tragen Sie hier das Kennwort des Benutzers ein.

Um SNMPv3 für den Benutzer zu aktivieren, muss das für den Benutzer konfigurierte Kennwort eine Mindestlänge von 8 Zeichen haben.

*Kennwort bestätigen*

Wiederholen Sie hier zur Bestätigung die Eingabe des Kennworts.

*Beschreibung*

Tragen Sie hier eine allgemeine Beschreibung des konfigurierten Benutzers ein.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Privilegien und Berechtigungen - Benutzerprivilegien und Benutzerberechtigungen konfigurieren

Mit der Gruppe *Privilegien und Berechtigungen* konfigurieren Sie die Kanal-spezifischen Benutzerprivilegien sowie die Kanal-unabhängigen Berechtigungen.

Bild 175: Benutzer '<name>' Konfiguration - Privilegien und Berechtigungen

*IPMI-Benutzer aktiviert*
: Wenn diese Option deaktiviert ist, kann sich der Benutzer nicht beim iRMC S4 anmelden.

*LAN Kanal Privileg*
: Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den LAN-Kanal zu:

  - *User*
  - *Operator*
  - *Administrator*
  - *OEM*

  Zum Berechtigungsumfang der einzelnen Berechtigungsgruppen siehe Abschnitt "Benutzerberechtigungen" auf Seite 65.

*Serieller Kanal Privileg*
: Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den seriellen Kanal zu. Zur Auswahl stehen die gleichen Berechtigungsgruppen wie unter *LAN Kanal Privileg*.

Ergänzend zu den Kanal-spezifischen Privilegien können Sie einem Benutzer individuell folgende Kanal-unabhängigen Berechtigungen erteilen:

*Benutzerkonfiguration erlaubt*
: Berechtigung zum Konfigurieren von lokalen Benutzerzugangsdaten.

*iRMC S4-Einstellungen konfigurieren*
: Berechtigung zum Konfigurieren der iRMC-Einstellungen.

*Konsolenumleitung erlaubt*
: Berechtigung zur Nutzung der Grafischen Konsolen-Umleitung (Advanced Video Redirection, AVR) im „Nur Lesen“- und „Volle Kontrolle“-Modus.

*Remote Storage erlaubt*
: Berechtigung zur Nutzung der Remote Storage-Funktionalität.

*Benutzer Interface (Text Zugang)*
: Wählen Sie hier die gewünschte Text-basierte Benutzerschnittstelle aus. Die folgenden Optionen stehen zur Verfügung:

  – *SMASH CLP*
    Siehe Abschnitt "Start a Command Line shell... - SMASH CLP Shell starten" auf Seite 406.

  – *Remote Manager*
    Siehe Kapitel "iRMC S4 über Telnet/SSH (Remote Manager)" auf Seite 387.

  – *Keine*

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### SNMPv3 Konfiguration

In der Gruppe *SNMPv3 Konfiguration* können Sie den iRMC S4-Benutzer für SNMPv3 konfigurieren. Im Vergleich zu SNMPv1/v2c stellt SNMPv3 eine höhere Sicherheitsstufe bereit, indem die SNMP-Pakete authentifiziert und verschlüsselt werden.

Die Parameter der Gruppe *SNMPv3 Konfiguration* sind deaktiviert (ausgegraut), wenn auf der Seite *SNMP Konfiguration* die Option *SNMP aktiviert* deaktiviert ist (siehe Abschnitt "SNMP Allgemeine Konfiguration" auf Seite 286).

Um SNMPv3 für den Benutzer zu aktivieren, muss das für diesen Benutzer konfigurierte Kennwort eine Mindestlänge von 8 Zeichen haben.

Auch wenn es Ihnen der SNMPv3-Standard erlaubt, SNMPv3 "ohne Authentfizierung und ohne Verschlüsselung (*noAuthnoPriv*)" oder "mit Authentifizierung, aber ohne Verschlüsselung (*AuthnoPriv*)" zu konfigurieren, erlaubt Ihnen die Gruppe *SNMPv3 Konfiguration* aus Sicherheitsgründen nur eine Konfiguration "mit Authentifizierung und mit Verschlüsselung (*AuthPriv*)" (siehe unten).

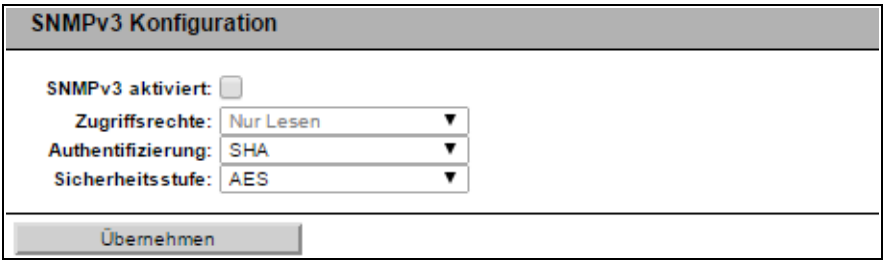



Bild 176: Seite Benutzer Verwaltung - Benutzer '<name>' Konfiguration, SNMPv3 Konfiguration

*SNMPv3 aktiviert*
Aktiviert den SNMPv3-Support für den Benutzer.

*Zugriffsrechte*
Zugriffsrechte des Benutzers. Derzeit ist *Nur Lesen* fest vorgegeben.

*Authentifizierung*
Wählen Sie das Authentifizierungsprotokoll aus, das SNMPv3 zur Authentfizierung verwendet.

*SHA*
SHA (Secure Hash Algorithm) wird zur Authentfizierung verwendet.

*MD5*
MD5 (Message-Digest Algorithm) wird zur Authentfizierung verwendet.

*Sicherheitsstufe*
Wählen Sie das Sicherheitsprotokoll aus, das SNMPv3 zur Verschlüsselung des SNMPv3-Datenverkehrs verwendet.

*DES*

DES (Digital Encryption Standard) wird zur Verschlüsselung des SNMPv3-Datenverkehrs verwendet.

*AES*

Die AES (Advanced Encryption Standard) 128-Bit-Verschlüsselung wird zur Verschlüsselung des SNMPv3-Datenverkehrs verwendet.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen

Mit der Gruppe *Öffentlichen SSHv2 Schlüssel für Benutzer aus Datei hochladen* können Sie für den zu konfigurierenden Benutzer einen öffentlichen SSHv2-Schlüssel aus einer Datei hochladen.

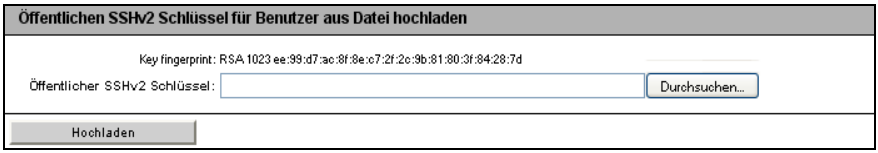



Bild 177: Benutzer '<name>' Konfiguration - Öffentlichen SSHv2-Schlüssel hochladen

*Durchsuchen...*

Öffnet einen Datei-Browser, über den Sie zur Datei mit dem öffentlichen SSHv2-Schlüssel navigieren können.

*Hochladen*

Lädt den im Eingabefeld angegebenen öffentlichen SSHv2-Schlüssel auf den iRMC S4.

Weitere Informationen zur Authentifizierung mit öffentlichem SSHv2-Schlüssel für iRMC S4-Benutzer finden Sie unter Abschnitt "SSHv2 Public Key-Authentifizierung für lokale iRMC S4-Benutzer" auf Seite 69.

### S/MIME-Zertifikat

In der Gruppe *S/MIME Zertifikat aus Datei hochladen* können Sie ein S/MIME-Zertifikat aus einer lokalen Datei laden.

> In Verbindung mit S/MIME unterstützt der iRMC S4 nur die Verschlüsselung. Die Signatur wird nicht unterstützt.

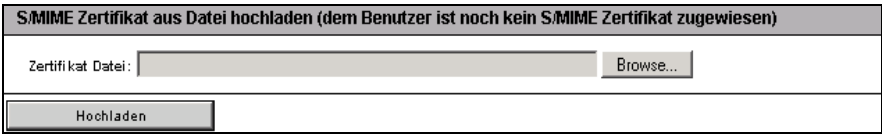

S/MIME Zertifikat aus Datei hochladen (dem Benutzer ist noch kein S/MIME Zertifikat zugewiesen)
Zertifikat Datei:
Browse...
Hochladen

Bild 178: Benutzer Verwaltung – Seite "Benutzer "<name>" Konfiguration", S/MIME-Zertifikat aus Datei hochladen

*Durchsuchen...*
: Öffnet einen Datei-Browser, über den Sie zur Datei mit dem öffentlichen SSHv2-Schlüssel navigieren können.

*Hochladen*
: Lädt das ausgewählte S/MIME-Zertifikat hoch.

Nach dem Hochladen des S/MIME-Zertifikats wird die Gruppe *S/MIME Zertifikat aus Datei hochladen* wie folgt angezeigt:

Bild 179: Benutzer Verwaltung – Seite "Benutzer "<name>" Konfiguration", S/MIME-Zertifikat wurde aus Datei hochgeladen

*Zertifikat ansehen*

Zeigt das S/MIME-Zertifikat bis zum nächsten Aktualisierungszyklus oder bis zur nächsten manuellen Aktualisierung der iRMC S4-Weboberfläche an.

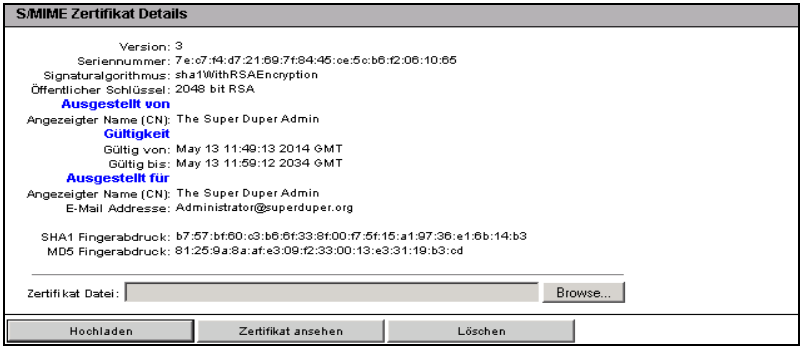



Bild 180: Benutzer Verwaltung – Seite "Benutzer "<name>" Konfiguration", S/MIME-Zertifikat – Zertifikat ansehen

*Löschen*

Löscht das S/MIME-Zertifikat vom iRMC S4.

### E-Mail Konfiguration - Benutzer-spezifische E-Mail-Einstellungen konfigurieren

Mit der Gruppe *E-Mail Konfiguration* konfigurieren Sie die Benutzer-spezifischen Einstellungen für das E-Mail-Format.

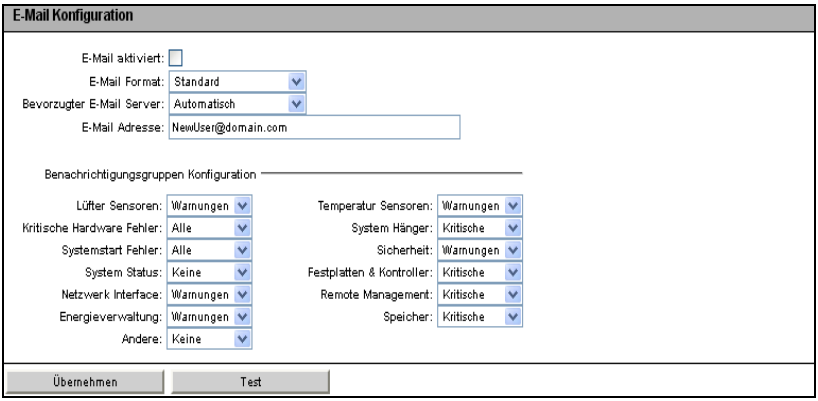



Bild 181: Seite Benutzer Verwaltung - Benutzer '<name>' Konfiguration, E-Mail Konfiguration

*E-Mail aktiviert*

Hier stellen Sie ein, ob der Benutzer per E-Mail über die Systemzustände informiert werden soll.

*Encrypted*

Legen Sie fest, ob E-Mails mit S/MIME verschlüsselt werden sollen.

*E-Mail Format*

Abhängig vom gewählten Mail-Format können Sie in der Seite *E-Mail Benachrichtigung (Gruppe Mail Format dependent Configuration* (siehe Seite 296) unterschiedliche Einstellungen vornehmen.

Folgende Mail-Formate stehen zur Verfügung:

- *Standard*
- *Fixed Subject*
- *ITS-Format*
- *SMS-Format*

Nur zur Erstellung von E-Mails mit einer maximalen Länge von 160 Zeichen. *SMS-Format* ist die bevorzugte SMS-Gateway-Lösung für E-Mails.

*Bevorzugter E-Mail Server*

Bevorzugter Mail Server.
Sie können zwischen folgenden Optionen wählen:

– *Automatisch*

  Falls die E-Mail nicht sofort erfolgreich versendet werden kann, weil z. B. der erste Mail-Server nicht verfügbar ist, wird E-Mail an den zweiten Mail-Server gesendet.

– *Erster*

  Nur der als Erster SMTP Server (siehe Seite 293) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

– *Zweiter*

  Nur der als Zweiter SMTP Server (siehe Seite 295) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

Fehler beim Versenden der E-Mail erzeugen einen Eintrag im Fehlerspeicher.

*E-Mail Adresse*

E-Mail-Adresse des Empfängers.

*Spezielle SMS-E-Mail-Betreffs verwenden*

Wird nur angezeigt, wenn *Mail Format: SMS-Format* aktiviert ist.

Wenn aktiviert, wird ein für den SMS-Gateway-Provider spezifischer E-Mail-Betreff verwendet.

*SMS-E-Mail-Betreff* (Nur wenn *Mail Format: SMS-Format* aktiviert ist.)

Für den SMS-Gateway-Provider spezifischer E-Mail-Betreff.

*Benachrichtigungsgruppen Konfiguration*

Hier können Sie Systemereignisse konfigurieren, über die ein iRMC S4-Benutzer per E-Mail benachrichtigt werden soll.

Jeder Eintrag im Fehlerspeicher (Eventlog-Eintrag) des iRMC S4 wird einer bestimmten Benachrichtigungsgruppe zugeordnet.

Für jede Benachrichtigungsgruppe sind folgende Einstellungen möglich:

*Keine*

Die Benachrichtigungsfunktion für diese Benachrichtigungsgruppe ist deaktiviert.

*Kritische*

Der iRMC S4 benachrichtigt den Benutzer per E-Mail, wenn ein Fehlerspeicher-Eintrag die Ereignisklasse *Kritisch* meldet.

*Warnung*

Der iRMC S4 benachrichtigt den Benutzer per E-Mail, wenn ein Fehlerspeicher-Eintrag ein Ereignis der Klassen *Leichte Fehler*, *Schwere Fehler* oder *Kritische Fehler* meldet.

*Alle*

Der iRMC S4 benachrichtigt den Benutzer über jedes zu einem Eintrag in den Fehlerspeicher führende Ereignis in dieser Benachrichtigungsgruppe.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

## 7.15.2 Verzeichnisdienst Konfiguration (LDAP) - Verzeichnisdienst am iRMC S4 konfigurieren

Für die globale Benutzerverwaltung über einen Verzeichnisdienst (Directory Service) müssen Sie den iRMC S4 mithilfe der Seite *Verzeichnisdienst Konfiguration* entsprechend konfigurieren.

Derzeit wird Unterstützung für iRMC S4 LDAP-Zugriff für die folgenden Verzeichnisdienste geboten: Microsoft Active Directory, Novell eDirectory und Open LDAP.

Die folgenden Zeichen sind in LDAP als Metazeichen für Such-Strings reserviert: *, \ , &, |, !, =, <, >, ~, :

Verwenden Sie diese Zeichen deshalb nicht als Bestandteil von Relative Distinguished Names (RDN).

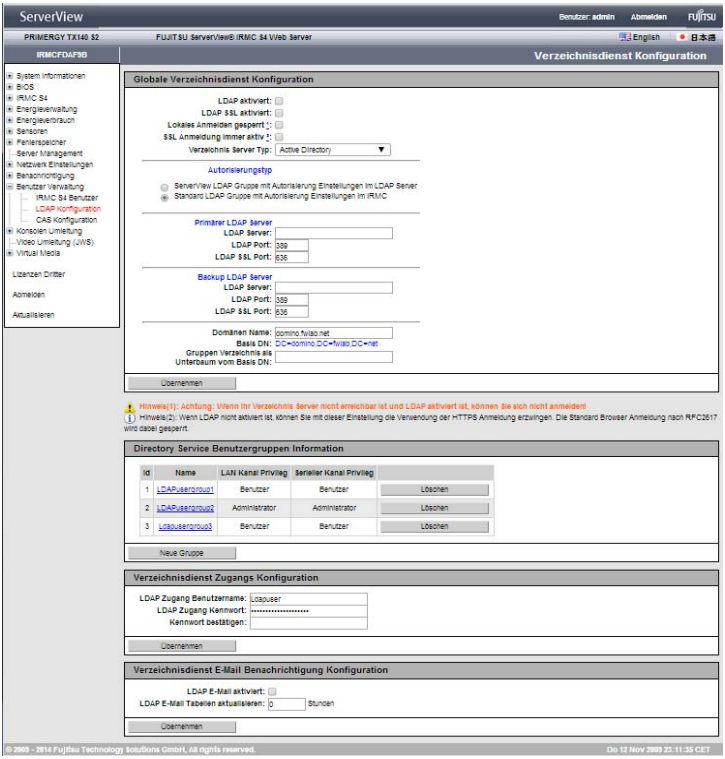



Bild 182: Seite Verzeichnisdienst Konfiguration (LDAP-Konfiguration)

*LDAP aktiviert*

Mit dieser Option legen Sie fest, ob der iRMC S4 via LDAP auf einen Verzeichnisdienst zugreifen kann. Der Verzeichnisdienst via LDAP kann nur genutzt werden, wenn *LDAP aktiviert* aktiviert ist.

Wenn *LDAP aktiviert* aktivier ist, dann werden die Anmeldeinformationen (siehe Seite 134) immer SSL-verschlüsselt zwischen dem Webbrowser und dem iRMC S4 übertragen.

*LDAP SSL aktiviert*

Wenn Sie diese Option aktivieren, erfolgt der Datenaustausch zwischen iRMC S4 und Verzeichnisserver (Directory Server) SSL-verschlüsselt.

*LDAP SSL aktiviert* hat keinen Einfluss darauf, ob die Seiten der iRMC S4-Weboberfläche SSL-gesichert geöffnet werden oder nicht.

*LDAP SSL aktiviert* sollten Sie nur aktivieren, wenn ein Domänencontroller-Zertifikat (Domain Controller-Zertifikat) installiert ist.

*Lokales Anmelden gesperrt*

Wenn Sie diese Option aktivieren, werden alle iRMC S4-lokalen Benutzerkennungen gesperrt, und nur die durch den Verzeichnisdienst verwalteten Benutzerkennungen sind gültig.

**ACHTUNG!**

Wenn die Option *Lokales Anmelden gesperrt* aktiviert ist und außerdem die Verbindung zum Verzeichnisdienst fehlschlägt, ist am iRMC S4 kein Anmelden mehr möglich.

*SSL Anmeldung immer aktiv*

Diese Option ist nur relevant, wenn gleichzeitig LDAP deaktiviert ist.

Wenn Sie diese Option aktivieren, wird stets die HTTP SSL-gesicherte Anmelde-Seite verwendet, auch wenn LDAP deaktiviert ist. Nur wenn Sie *SSL Anmeldung immer aktiv* nicht aktivieren und außerdem LDAP deaktiviert ist, kommt eine über Digest Authentication Login gesicherte Maske zum Einsatz.

*Verzeichnis Server Typ*

Typ des verwendeten Verzeichnisservers.

Folgende Verzeichnisdienste werden unterstützt:

– *Active Directory*: Microsoft Active Directory

– *Novell*: Novell eDirectory

– *OpenLDAP*: OpenLDAP

– *Open DS / Open DJ / Apache DS*

*Authentifizierungsart*

Verwendete Authentifizierungsart.

*ServerView LDAP Gruppe mit Autorisierung Einstellungen im LDAP Server*

ServerView-spezifische LDAP-Gruppen mit Autorisierungseinstellungen in der *SVS*-Struktur auf dem LDAP-Server dienen zum Festlegen von Benutzerberechtigungen (siehe Handbuch "Benutzerverwaltung in ServerView").

*Standard LDAP Gruppe mit Autorisierung Einstellungen im iRMC*

Es wird keine ServerView-spezifische *SVS*-Struktur auf dem LDAP-Server verwendet. Stattdessen wird die Benutzerauthentifizierung mittels einer LDAP-Standardgruppe geprüft, der der Benutzer angehört. iRMC S4-spezifische Benutzerberechtigungen für diese LDAP-Standardgruppe müssen lokal auf dem iRMC S4 konfiguriert werden (siehe Abschnitt "LDAP-Standardgruppen mit Autorisierungseinstellungen auf dem iRMC S4" auf Seite 316).

Diese Methode unterstützt die Verschachtelung von Gruppen. Daher werden alle iRMC S4-spezifischen Benutzerberechtigungen, die Sie einer LDAP-Standardgruppe zuweisen, automatisch von den darin verschachtelten Gruppen übernommen.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

Je nach gewähltem Verzeichnisdienst werden unterschiedliche Eingabefelder angeboten:

– Zu *Active Directory* sieheAbschnitt "iRMC S4 für Microsoft Active Directory konfigurieren" auf Seite 323.

– Zu *eDirectory*, *Open LDAP* und *OpenDJ* sieheAbschnitt "iRMC für Novell eDirectory / OpenLDAP / OpenDS / Open DJ konfigurieren" auf Seite 328.

#### 7.15.2.1 LDAP-Standardgruppen mit Autorisierungseinstellungen auf dem iRMC S4

Wenn *Standard LDAP Gruppe mit Autorisierung Einstellungen im iRMC* auf der Seite *Verzeichnisdienst Konfiguration* aktiviert wurde, sind einige zusätzliche Einstellungen erforderlich, mit denen Sie die LDAP-Gruppen auf dem iRMC S4 verwalten können. Diese LDAP-Gruppen werden zum Definieren von iRMC S4-Rechten und -Berechtigungen für Benutzer verwendet, die den LDAP-Standardgruppen auf dem Verzeichnisserver angehören.

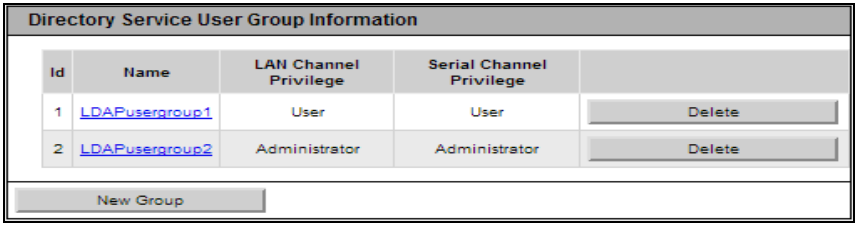



Bild 183: Microsoft Active Directory Informationen über die Verzeichnisdienst-Benutzergruppe

*Löschen*

Löscht die entsprechenden Benutzergruppeninformationen.

*Neue Gruppe*

Öffnet die Gruppe *Neue LDAP Benutzer Gruppe*, mit der Sie die iRCM S4-Berechtigungen für eine neue LDAP-Gruppe definieren können:

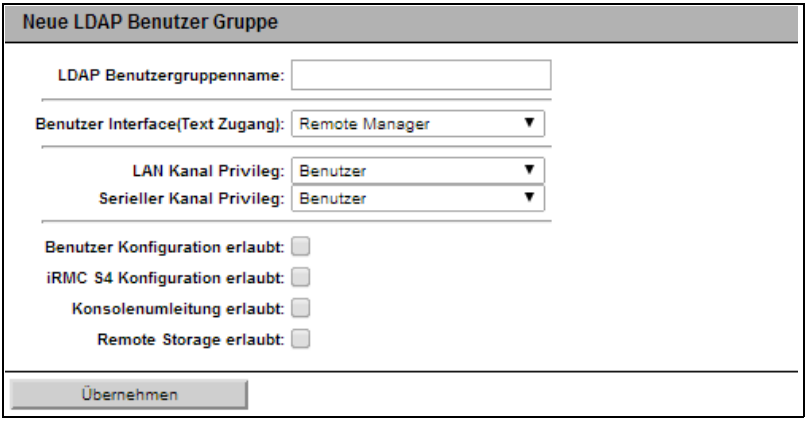



Bild 184: Microsoft Active Directory Neue LDAP Benutzergruppe

*LDAP Benutzergruppenname*

Name der neuen LDAP Benutzergruppe

*User Shell (Text Access)*

Wählen Sie hier die gewünschte Text-basierte Benutzerschnittstelle aus.
Die folgenden Optionen stehen zur Verfügung:

- *SMASH CLP*
  Siehe Abschnitt "Start a Command Line shell... - SMASH CLP Shell starten" auf Seite 406.
- *Remote Manager*
  Siehe Kapitel "iRMC S4 über Telnet/SSH (Remote Manager)" auf Seite 387.
- *Keine*

*LAN Kanal Privileg*

Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den LAN-Kanal zu:

- *User*
- *Operator*
- *Administrator*
- *OEM*

Zum Berechtigungsumfang der einzelnen Berechtigungsgruppen siehe Abschnitt "Benutzerberechtigungen" auf Seite 65.

*Serieller Kanal Privileg*

Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe für den seriellen Kanal zu. Zur Auswahl stehen die gleichen Berechtigungsgruppen wie unter *LAN Kanal Privileg*.

*Benutzerkonfiguration erlaubt*

Berechtigung zum Konfigurieren von lokalen Benutzerzugangsdaten.

*iRMC S4-Einstellungen konfigurieren*

Berechtigung zum Konfigurieren der iRMC S4-Einstellungen

*Konsolenumleitung erlaubt*

Berechtigung zur Nutzung der Grafischen Konsolen-Umleitung (Advanced Video Redirection, AVR) im „Nur Lesen“- und „Volle Kontrolle“-Modus.

*Remote Storage erlaubt*

Berechtigung zur Nutzung der *Virtual Media*-Funktionalität

*<Name>*

Wenn Sie auf einen Link in der Spalte *Name* klicken, wird eine neue Seite geöffnet, über die Sie die Konfigurationseinstellungen der entsprechenden LDAP-Benutzergruppe ändern und/oder ergänzen können:

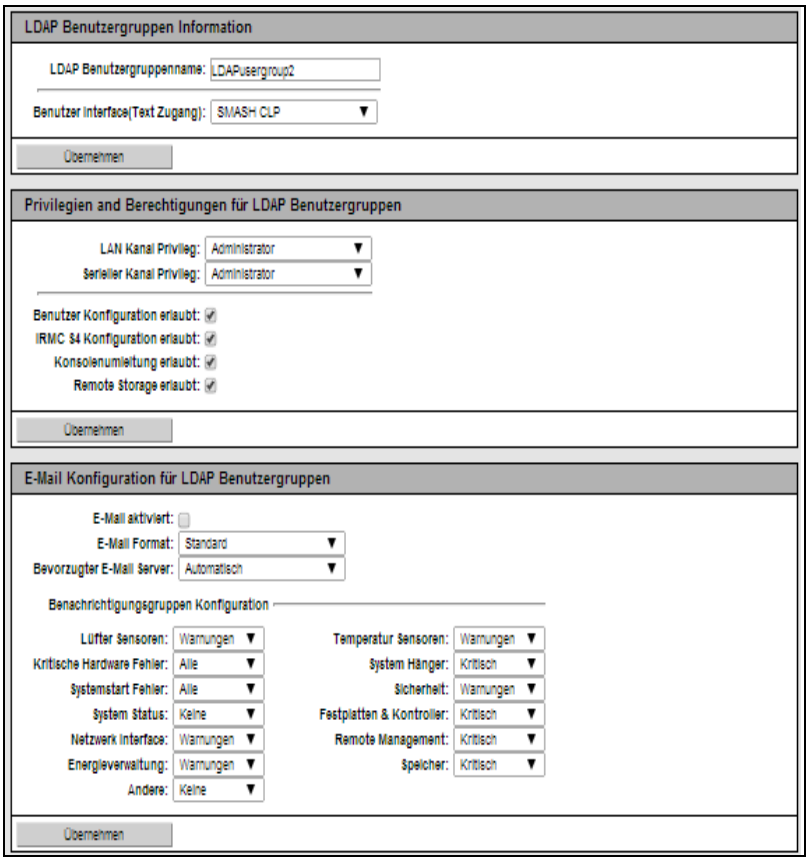



Bild 185: Microsoft Active Directory Informationen über die Verzeichnisdienst-Benutzergruppe

Die Optionen unter *LDAP Benutzergruppen Information* und *Privilegien and Berechtigungen für LDAP Benutzergruppen* entsprechen den unter der Option *Neue Gruppe* beschriebenen (siehe Seite 316).

Die Optionen für *E-Mail Konfiguration für LDAP Benutzergruppen* lauten folgendermaßen:

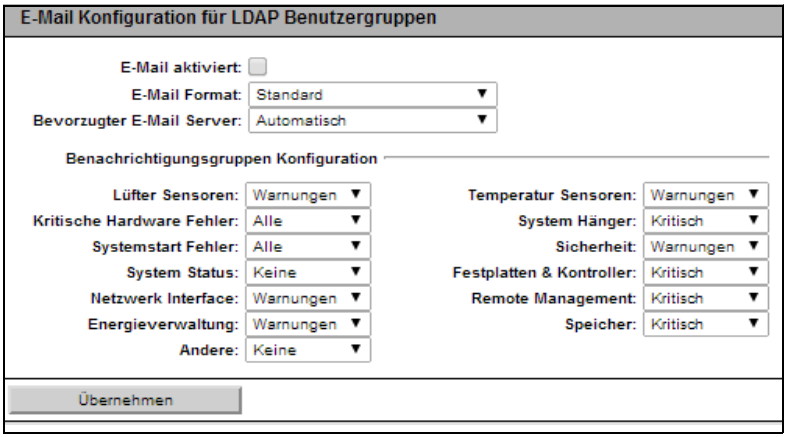



Bild 186: Microsoft Active Directory Informationen über die Verzeichnisdienst-Benutzergruppe

*E-Mail aktiviert*

Hier stellen Sie ein, ob der Benutzer per E-Mail über die Systemzustände informiert werden soll.

*E-Mail Format*

Abhängig vom gewählten Mail-Format können Sie in der Seite *E-Mail Benachrichtigung (Gruppe Mail Format dependent Configuration* (siehe Seite 296) unterschiedliche Einstellungen vornehmen.

Folgende Mail-Formate stehen zur Verfügung:

- *Fixed Subject*
- *ITS-Format*
- *SMS-Format*

*Bevorzugter E-Mail Server*

Bevorzugter Mail Server.
Sie können zwischen folgenden Optionen wählen:

– *Automatisch*

  Falls die E-Mail nicht sofort erfolgreich versendet werden kann, weil z. B. der erste Mail-Server nicht verfügbar ist, wird E-Mail an den zweiten Mail-Server gesendet.

– *Erster*

  Nur der als Erster SMTP Server (siehe Seite 293) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

– *Zweiter*

  Nur der als Zweiter SMTP Server (siehe Seite 295) konfigurierte Mail Server wird als bevorzugter Mail Server verwendet.

Fehler beim Versenden der E-Mail erzeugen einen Eintrag im Fehlerspeicher.

*E-Mail Adresse*

E-Mail-Adresse des Empfängers.

Die E-Mail-Adresse muss für den Benutzer im LDAP-Verzeichnis konfiguriert sein.

*Benachrichtigungsgruppen Konfiguration*

Hier können Sie Systemereignisse konfigurieren, über die ein iRMC S4-Benutzer per E-Mail benachrichtigt werden soll. Jeder Eintrag im Fehlerspeicher (Eventlog-Eintrag) des iRMC S4 wird einer bestimmten Benachrichtigungsgruppe zugeordnet.

Für jede Benachrichtigungsgruppe sind folgende Einstellungen möglich:

– *Keine*

  Die Benachrichtigungsfunktion für diese Benachrichtigungsgruppe ist deaktiviert.

– *Kritische*

  Der iRMC S4 benachrichtigt den Benutzer per E-Mail, wenn ein Fehlerspeicher-Eintrag die Ereignisklasse *Kritisch* meldet.

– *Warnung*

  Der iRMC S4 benachrichtigt den Benutzer per E-Mail, wenn ein Fehlerspeicher-Eintrag ein Ereignis der Klassen *Leichte Fehler*, *Schwere Fehler* oder *Kritische Fehler* meldet.

– *Alle*

  Der iRMC S4 benachrichtigt den Benutzer über jedes zu einem Eintrag in den Fehlerspeicher führende Ereignis in dieser Benachrichtigungsgruppe.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### 7.15.2.2 iRMC S4 für Microsoft Active Directory konfigurieren

Nachdem Sie Ihre Wahl *Active Directory* mit *Übernehmen* haben, wird die folgende Variante der Seite *Verzeichnisdienst Konfiguration* angezeigt:

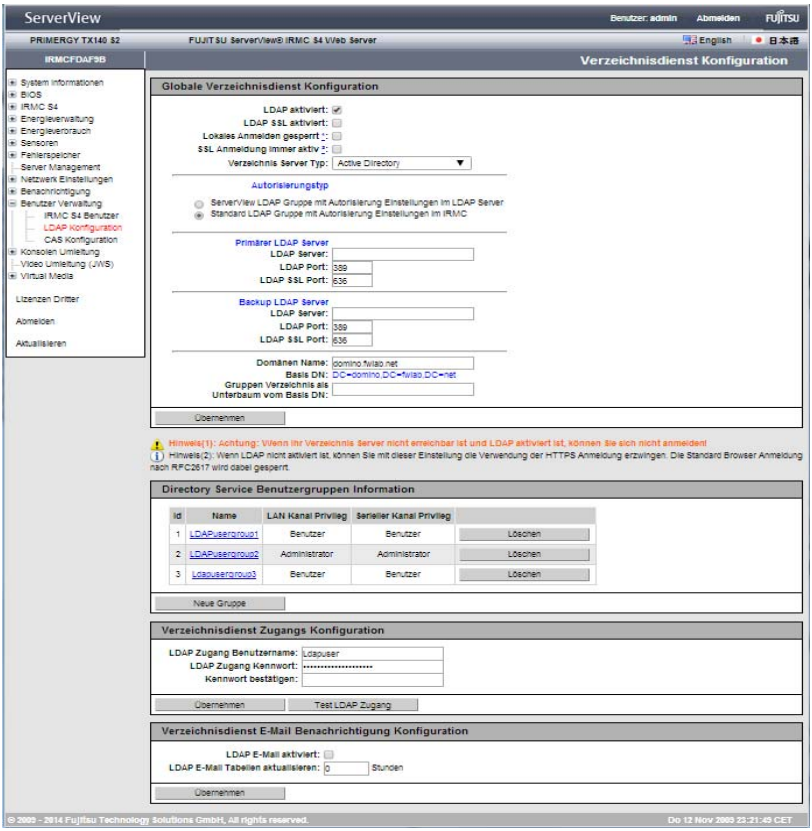



Bild 187: Verzeichnisdienst Konfiguration: Spezifikationen für Microsoft Active Directory

Die als Beispiele in Bild 187 aufgeführten Einträge beziehen sich auf die Beispiele und Abbildungen im Handbuch „Benutzerverwaltung in ServerView“.

Gehen Sie wie folgt vor:

► Vervollständigen Sie Ihre Angaben Sie in der Gruppe *Globale Verzeichnisdienst Konfiguation*:

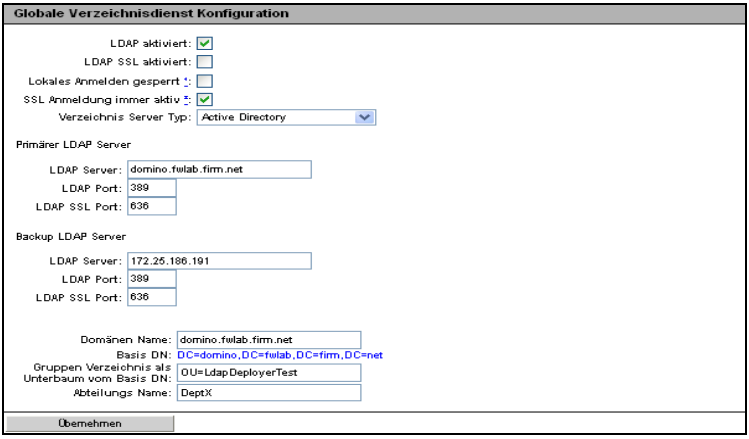



Bild 188: Globale Verzeichnisdienst Konfiguration: Spezifikationen für Microsoft Active Directory

*Primärer LDAP Server*

LDAP Verzeichnisserver, der verwendet werden soll.

*LDAP Server*

IP-Adresse oder DNS-Name des primären Verzeichnisservers.

*LDAP Port*

LDAP-Port des primären Verzeichnisservers.

*LDAP SSL Port*

Sicherer LDAP-Port des primären Verzeichnisservers.

*Backup LDAP Server*

LDAP Verzeichnisserver, der als Backup-Server geführt und bei Ausfall des *primären LDAP Servers* als Verzeichnisserver herangezogen wird.

*LDAP Server*

IP-Adresse oder DNS-Name des Backup LDAP Verzeichnisservers.

*LDAP Port*
LDAP-Port des Backup LDAP Verzeichnisservers.

*LDAP SSL Port*
Sicherer LDAP-Port des Backup LDAP Verzeichnisservers.

*Domänen Name*
Vollständiger DNS-Pfadname des Verzeichnisservers.

*Basis DN*
*Basis DN* wird automatisch von *Domänen Name* abgeleitet.

*Gruppen Verzeichnis als Unterbaum vom Basis DN*
Pfadname der Organisationseinheit (OU) der als Teilbaum des *Basis DN* (Group DN Context) die OUs *SVS* oder *iRMCgroups* enthält.

*Abteilungs Name*

Diese Option wird nur angezeigt, wenn die Option *Standard LDAP Gruppe mit Autorisierung Einstellungen im iRMC* aktiviert wurde.

Der Abteilungsname wird im Verzeichnisdienst zur Bestimmung der Benutzerrechte und Benachrichtigungsgruppen (Alert Roles) benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

- Konfigurieren Sie die iRMC-lokalen Benutzergruppendaten in der Gruppe *LDAP User Group Information*:

Die Gruppe *LDAP User Group Information* wird nur angezeigt, wenn die Option *Standard LDAP Gruppe mit Autorisierung Einstellungen im iRMC* aktiviert wurde.

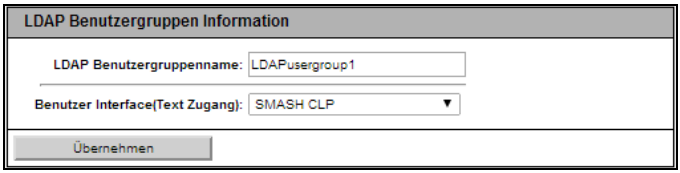



Bild 189: Microsoft Active Directory LDAP User Group Information

Zu Einzelheiten siehe Abschnitt "LDAP-Standardgruppen mit Autorisierungseinstellungen auf dem iRMC S4" auf Seite 316.

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Konfigurieren Sie den LDAP-Zugang in der Gruppe *Verzeichnisdienst Zugangs Konfiguation* group:

Die hier vorzunehmenden Einstellungen werden für die Alarm-Benachrichtigung (Alerting) im Zusammenhang mit globalen Benutzerkennungen benötigt. Falls die Alarmbenachrichtigung nicht aktiviert ist, sind die Einstellungen der Gruppe *Verzeichnisdienst Zugangs Konfiguation* nicht relevant.

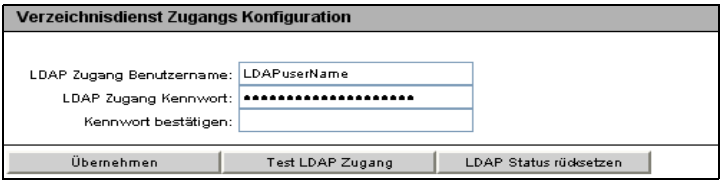



Bild 190: Microsoft Active Directory Verzeichnisdienst Zugangs Konfiguration:

*LDAP Zugang Benutzername*

Benutzername, unter dem sich der iRMC S4 beim LDAP-Server anmeldet.

*LDAP Zugang Kennwort*

Kennwort, mit dem sich der Benutzername beim LDAP-Server authentisiert.

*Kennwort bestätigen*

Wiederholen Sie das unter *LDAP Zugang Kennwort* eingegebene Kennwort.

*Test LDAP Zugang*

Überprüft die Zugangsdaten zum LDAP-Verzeichnisserver und zeigt als Ergebnis den LDAP-Status an (siehe Bild 191).

Dieser Test prüft lediglich die Basis-Zugangsdaten („LDAP-Server vorhanden?“, „Benutzer konfiguriert?“), führt jedoch keine vollständige Autorisierung des Benutzers durch.

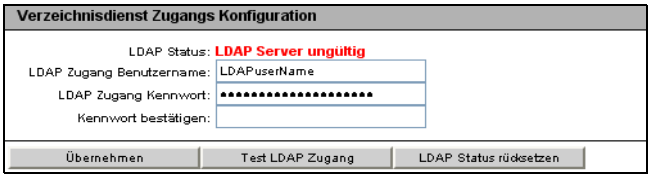



Bild 191: Microsoft Active Directory Status der Verbindung zum LDAP-Server

- ► Klicken Sie auf *LDAP Status zurücksetzen*, um die Statusanzeige zurückzusetzen.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Konfigurieren Sie in der Gruppe *Verzeichnisdienst E-Mail Benachrichtigung Konfiguration* die Einstellungen für globale E-Mail-Benachrichtigung.

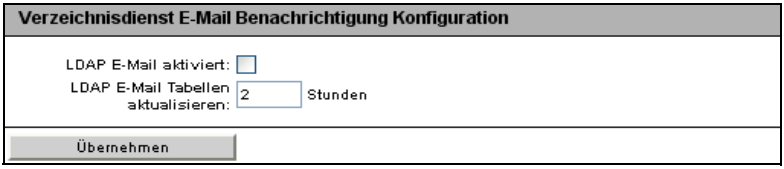



Bild 192: Verzeichnisdienst E-Mail Benachrichtigung Konfiguration

*LDAP E-Mail aktiviert*

Aktiviert die globale E-Mail-Benachrichtigung.

*LDAP E-Mail Tabellen aktualisieren [Stunden]*

Definiert das Intervall für die regelmäßige Aktualisierung der E-Mail-Tabelle (siehe Handbuch "Benutzerverwaltung in ServerView").

Es wird dringend empfohlen, einen Wert >0 anzugeben. Der Wert “0” hat zur Folge, dass die Tabelle nicht regelmäßig aktualisiert wird.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### 7.15.2.3 iRMC für Novell eDirectory / OpenLDAP / OpenDS / Open DJ konfigurieren

Nachdem Sie Ihre Wahl *Novell* oder *OpenLDAP* mit *Übernehmen* bestätigt haben, wird die nachfolgend beschriebene Variante der Seite *Verzeichnisdienst Konfiguration* angezeigt:

Der Aufbau der Seite *Verzeichnisdienst Konfiguration* ist für Novell eDirectory, OpenLDAP und OpenDS/OpenDJ identisch.

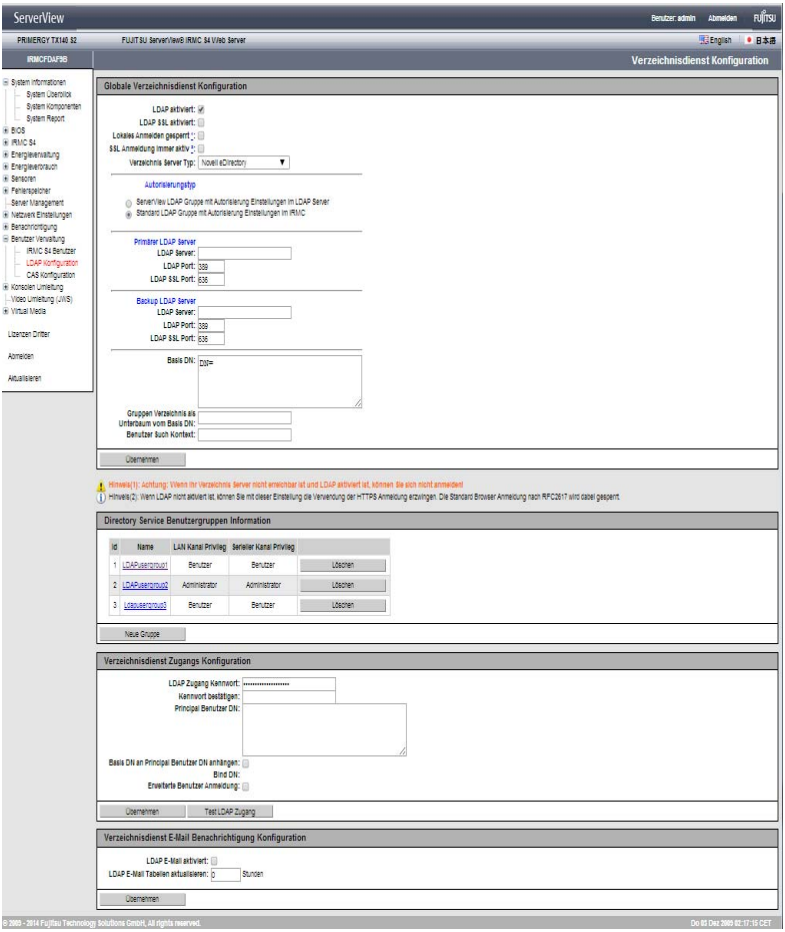



Bild 193: Globale Verzeichnisdienst Konfiguration: Spezifikationen für Novell eDirectory / Open LDAP

Gehen Sie wie folgt vor:

► Vervollständigen Sie Ihre Angaben Sie in der Gruppe *Globale Verzeichnisdienst Konfiguation*:

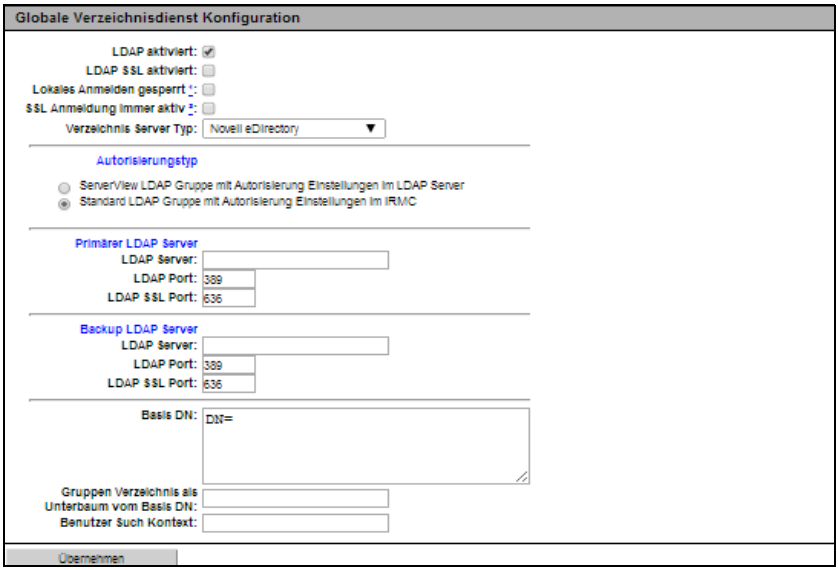



Bild 194: Globale Verzeichnisdienst Konfiguration: Spezifikationen für Novell eDirectory / Open LDAP / OpenDS / Open DJ

*Primärer LDAP Server*

LDAP Verzeichnisserver, der verwendet werden soll.

*LDAP Server*

IP-Adresse oder DNS-Name des primären Verzeichnisservers.

*LDAP Port*

LDAP-Port des primären Verzeichnisservers.

*LDAP SSL Port*

Sicherer LDAP-Port des primären Verzeichnisservers.

*Backup LDAP Server*

LDAP Verzeichnisserver, der als Backup-Server geführt und bei Ausfall des *primären LDAP Servers* als Verzeichnisserver herangezogen wird.

*LDAP Server*

IP-Adresse oder DNS-Name des Backup LDAP Verzeichnisservers.

*LDAP Port*

LDAP-Port des Backup LDAP Verzeichnisservers.

*LDAP SSL Port*

Sicherer LDAP-Port des Backup LDAP Verzeichnisservers.

*Abteilungs Name*

Diese Option wird nur angezeigt, wenn die Option *Standard LDAP Gruppe mit Autorisierung Einstellungen im iRMC* aktiviert wurde.

Der Abteilungsname wird im Verzeichnisdienst zur Bestimmung der Benutzerrechte benötigt. Ein Benutzer kann für den Server der Abteilung X andere Rechte besitzen als für den Server der Abteilung Y.

*Basis DN*

Der *Basis DN* (Base DN) ist der „vollständig eindeutige Name“ (Fully Distinguished Name) des eDirectory oder OpenLDAP Servers und repräsentiert den Baum oder Teilbaum, in dem die Organisationseinheit (Organizational Unit, OU) *SVS* oder *iRMCgroups* enthalten ist. Dieser DN bildet den Ausgangspunkt für LDAP-Suchoperationen.

*Gruppen Verzeichnis als Unterbaum vom Basis DN*

Pfadname der Organisationseinheit (OU) der als Teilbaum des *Basis DN* (Group DN Context) die OU *SVS* enthält.

*Benutzer Such Kontext*

Startpunkt für die Suche nach Benutzern. Eine Benutzersuchkontext-Regel wird bei der Suche nach iRMC S4-Benutzern bewertet. Sie gibt einen gültigen LDAP Distinguished Name (DN) zurück, der als Basiskontext für die Benutzersuche dient.

*LDAP group scheme*

Schema für eine LDAP-Gruppe.

*LDAP member scheme*
Schema für einen LDAP-Benutzer.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Konfigurieren Sie die iRMC-lokalen Benutzergruppendaten in der Gruppe *LDAP Benutzergruppen Information*:

Die Gruppe *LDAP Benutzergruppen Information* wird nur angezeigt, wenn die Option *Standard LDAP Gruppe mit Autorisierung Einstellungen im iRMC* aktiviert wurde.

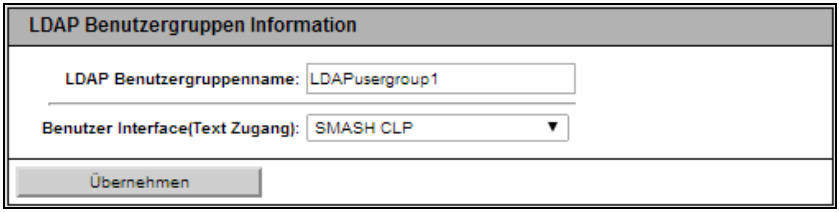



Bild 195: Microsoft Active Directory LDAP Benutzergruppen Information

Zu Einzelheiten siehe Abschnitt "LDAP-Standardgruppen mit Autorisierungseinstellungen auf dem iRMC S4" auf Seite 316.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Konfigurieren Sie den LDAP-Zugang in der Gruppe *Verzeichnisdienst Zugangs Konfiguration*:

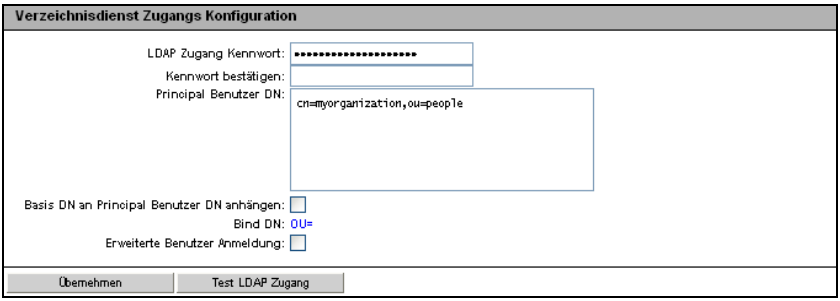



Bild 196: Novell eDirectory / Open LDAP: Verzeichnisdienst Zugangs Konfiguration:

*LDAP Zugang Kennwort*
Kennwort, mit dem sich der *Principal Benutzer* (Principal User) beim LDAP-Server authentisiert.

*Kennwort bestätigen*

Wiederholen Sie das unter *LDAP Zugang Kennwort* eingegebene Kennwort.

*Principal Benutzer DN*

„Fully Distinguished Name“, d.h.vollständige Beschreibung von Objektpfad und der Attributen der generischen iRMC S4-Benutzerkennung (Principal Benutzer), unter der der iRMC S4 vom LDAP-Server die Benutzerberechtigungen der iRMC S4-Benutzer erfragt.

*Basis DN an Principal Benutzer DN anhängen*

Wenn Sie diese Option aktivieren, brauchen Sie den Basis DN unter *Principal Benutzer DN*. Es wird dann der Basis DN verwendet, den Sie in der Gruppe *Globale Verzeichnisdienst* unter *Basis DN* spezifiziert haben.

*Bind DN*

Unter *Bind DN* wird der Principal Benutzer DN angezeigt, wie er für die LDAP-Authentifizierung verwendet wird.

*Erweiterte Benutzer Anmeldung*

Erhöhte Flexibilität bei der Benutzeranmeldung.

**ACHTUNG!**

Aktivieren Sie diese Option nur, wenn Sie mit der LDAP-Syntax vertraut sind. Wenn Sie versehentlich einen ungültigen Suchfilter spezifizieren und aktivieren, können sich Benutzer erst nach einer Deaktivierung der Option *Erweiterte BenutzerAnmeldung* wieder unter einer globalen Benutzerkennung am iRMC S4 anmelden.

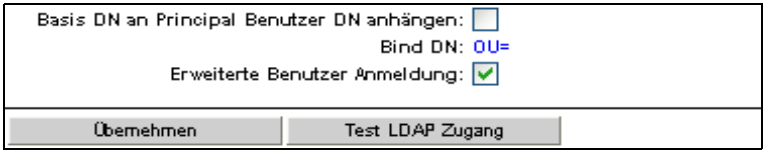



Bild 197: Erweiterte Benutzer Anmeldung

Wenn Sie *Erweiterte Benutzer* Anmeldung markieren und mit *Übernehmen* aktivieren, wird ein zusätzliches Eingabefeld *Benutzer Such Kriterium* angezeigt, das mit dem Standard-Anmelde-Suchfilter "(&(objectclass=person)(cn=%s))" vorbelegt ist.

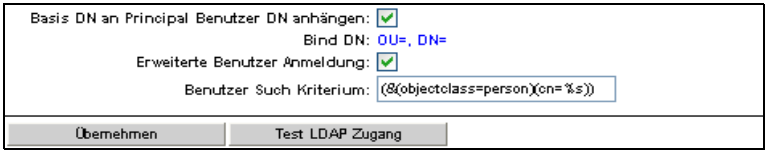



Bild 198: LDAP-Suchfilter für „Erweiterte Benutzer Anmeldung“

Beim Anmelden wird der Platzhalter „%s“ durch die jeweilige globale Benutzerkennung ersetzt. Den Standardfilter können Sie modifizieren, indem Sie z.B. anstatt „cn=“ ein anderes Attribut angeben. Anmeldeberechtigt am iRMC S4 sind dann alle globalen Benutzerkennungen, die den Bedingungen dieses Suchfilters genügen.

*Test LDAP Zugang*

Überprüft die Zugangsdaten zum LDAP-Verzeichnisserver und zeigt als Ergebnis den LDAP-Status an (siehe Bild 191).

Dieser Test prüft lediglich die Basis-Zugangsdaten („LDAP-Server vorhanden?“, „Benutzer konfiguriert?“), führt jedoch keine vollständige Autorisierung des Benutzers durch.

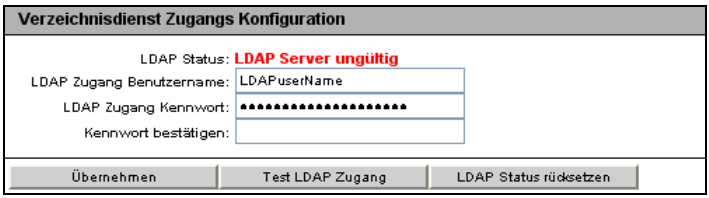



Bild 199: eDirectory / OpenLDAP: Status der Verbindung zum LDAP-Server

► Klicken Sie auf *LDAP Status zurücksetzen*, um die Statusanzeige zurückzusetzen.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

► Konfigurieren Sie in der Gruppe *Verzeichnisdienst E-Mail Benachrichtigung Konfiguration* die Einstellungen für globale E-Mail-Benachrichtigung.

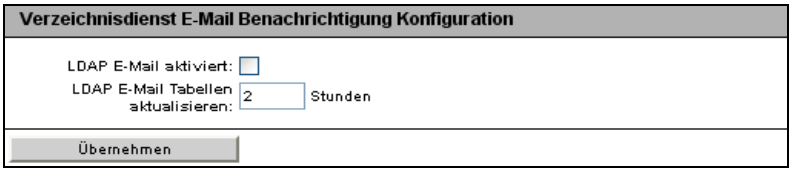



Bild 200: Verzeichnisdienst E-Mail Benachrichtigung Konfiguration

*LDAP E-Mail aktiviert*

Aktiviert die globale E-Mail-Benachrichtigung.

*LDAP E-Mail Tabellen aktualisieren [Stunden]*

Definiert das Intervall für die regelmäßige Aktualisierung der E-Mail-Tabelle (siehe Handbuch "Benutzerverwaltung in ServerView"). Der Wert “0” hat zur Folge, dass die Tabelle nicht regelmäßig aktualisiert wird.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

## 7.15.3 Centralized Authentication Service (CAS) Konfiguration - CAS Konfiguration

Diese Anzeige wird nicht von allen PRIMERGY Servern mit iRMC S4 unterstützt.

SSO wird nur für den Zugriff auf den iRMC S4 über die Weboberfläche unterstützt. SSO wird **nicht** für den Zugriff auf den iRMC S4 über den Remote Manager (Telnet/SSH) unterstützt

Über die Seite *Centralized Authentication Service (CAS) Konfiguration* können Sie die iRMC S4 Weboberfläche für die CAS-basierte Single sign-on (SSO)-Authentifizierung konfigurieren.

Wenn sich ein Benutzer das erste Mal bei einer Anwendung innerhalb der SSO-Domäne des CAS anmeldet, fordert ihn das CAS-spezifische Anmeldefenster zur Eingabe seiner Authentifizierungsdaten auf. Nach einmaliger erfolgreicher Authentifizierung durch den CAS Service hat der Benutzer dann Zugriff auf die iRMC S4-Weboberfläche sowie auf alle weiteren Services innerhalb der SSO-Domäne, ohne dass er jedes Mal erneut zur Eingabe seiner Authentisierungsdaten aufgefordert wird.

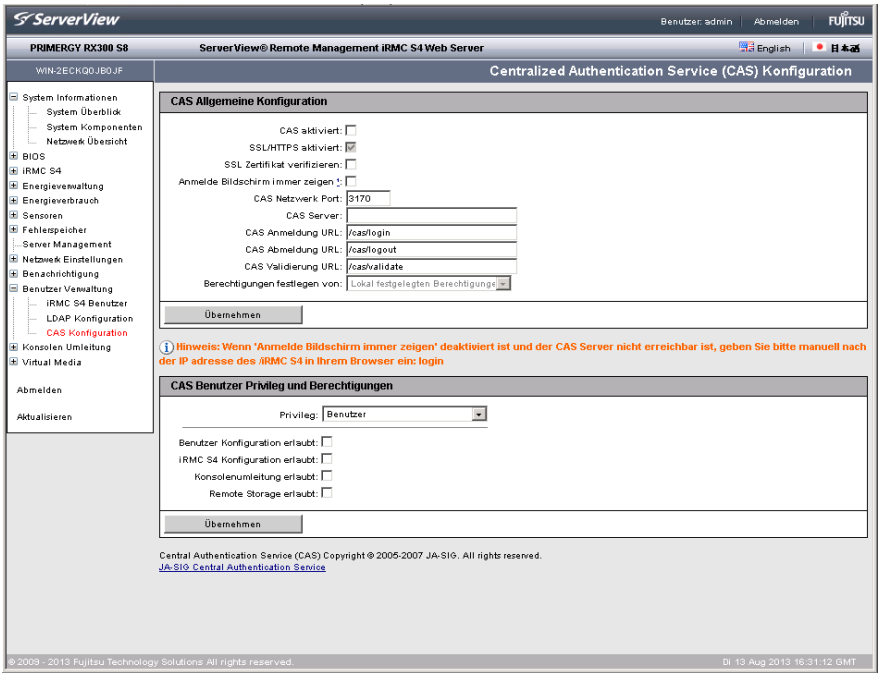



Bild 201: Centralized Authentication Service (CAS) Konfiguration

## CAS Allgemeine Konfiguration

Mit der Gruppe *CAS Allgemeine Konfiguration* können Sie die CAS-Zugriffsdaten konfigurieren.

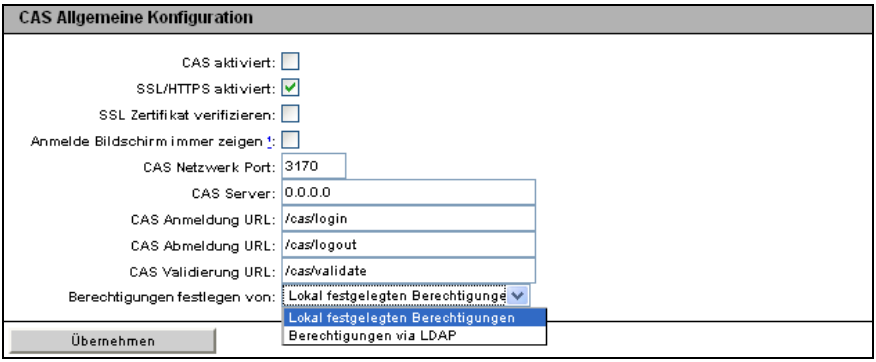



Bild 202: CAS Allgemeine Konfiguration

*CAS aktiviert*

Ermöglicht SSO beim Verwenden des CAS-Services, den Sie in der Gruppe *CAS Allgemeine Konfiguration* festlegen.

*SSL/HTTPS aktiviert*

Die gesamte Kommunikation zwischen dem CAS-Service und dem iRMC S4 wird mittels SSL verschlüsselt.

*SSL Zertifikat verifizieren*

Das SSL-Zertifikat des CAS-Services wird anhand des CA-Zertifikats überprüft.

*Anmelde Bildschirm immer zeigen*

Wenn *Anmelde Bildschirm immer zeigen* deaktiviert ist und der CAS-Service nicht erreichbar ist, geben Sie nach der IP-Adresse des iRMC S4 in der Browsernavigationsleiste `/login` ein.

Die iRMC S4-Anmeldeseite wird immer angezeigt:

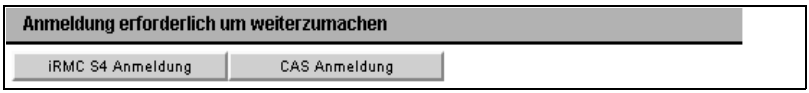



Bild 203: Anmeldeseite

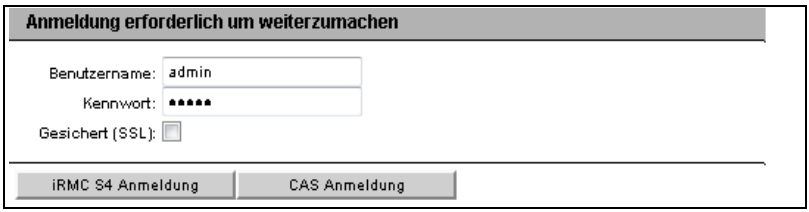



Bild 204: Anmeldeseite - explizite Authentifizierung erforderlich

Damit können Benutzer sich vorübergehend beim iRMC S4 mit Privilegien und Berechtigungen anmelden, die sich von dem unter *CAS Benutzer Privileg und Berechtigungen* festgelegten Autorisierungsprofil unterscheiden (siehe Seite 339)

Ein Benutzer kann beispielswiese mit einer Benutzerkennung am CAS-Service angemeldet sein und über das Privileg *Benutzer* verfügen. Er möchte jetzt jedoch eine Aktion ausführen, für die er das Privileg *Administrator* benötigt. Der Benutzer kann sich vorübergehend beim

iRMC S4 mit einer Benutzerkennung mit den erforderlichen Privilegien anmelden. Der Benutzer kann jedoch nicht zwischen den beiden Benutzerkennungen wechseln.

Die Schaltflächen *iRMC S4 Anmeldung* und *CAS Anmeldung* haben die folgende Funktionsweise:

*iRMC S4 Anmeldung*
: Der Benutzer wird mit den für *Benutzername* und *Kennwort* festgelegten Angaben bei der iRMC S4-Weboberfläche angemeldet. Der CAS-Service wird umgangen.

*CAS Anmeldung*
: Der Benutzer wird über SSO bei der iRMC S4-Weboberfläche angemeldet:

  – Falls der Benutzer noch nicht vom CAS-Service authentifiziert wurde:
    Der Benutzer wird an den CAS-Service umgeleitet, um mit den entsprechenden Angaben für *Benutzername* und *Kennwort* authentifiziert zu werden.

  – Falls der Benutzer bereits vom CAS-Service authentifiziert wurde:
    Der Benutzer wird beim iRMC S4 angemeldet, ohne nach Benutzername und Kennwort gefragt zu werden.

*CAS Netzwerk Port*
: Anschluss des CAS-Service.
Standard-Portnummer: 3170

*CAS Server*
: DNS-Name des CAS-Service.

Alle Systeme, die zur SSO-Domäne gehören, müssen die zentrale Management-Station (CMS) unbedingt über dieselbe Adressstruktur referenzieren. (Eine SSO-Domäne umfasst alle Systeme bei denen die Authentifizierung über denselben CAS Service abgewickelt wird). Falls Sie z. B. den ServerView Operations Manager unter Verwendung des Namens „my-cms.my-domain“ installiert haben, müssen Sie bei der Konfiguration des CAS-Service für einen iRMC S4 den identischen Namen verwenden. Geben Sie dagegen nur „my-cms“ oder eine andere IP-Adresse von my-cms an, wird die SSO-Funktionalität zwischen den beiden Systemen nicht aktiviert.

*CAS Anmeldung URL*
Anmeldungs-URL des CAS-Service.

*CAS Abmeldung URL*
Abmeldungs-URL des CAS-Service.

*CAS Validierung URL*
Validierungs-URL des CAS-Service.

*Berechtigungen festlegen von*
Definiert das iRMC S4-Privileg und die Berechtigungen für Benutzer, die mittels SSO beim iRMC S4 angemeldet sind.

*Lokal festgelegten Berechtigungen*
Das Privileg und die Berechtigungen, die unter *CAS Benutzer Privileg und Berechtigungen* festgelegt wurden, gelten für den Benutzer.

*Berechtigungen via LDAP*
Das im LDAP-Verzeichnisdienst definierte Autorisierungsprofil gilt für den Benutzer.

Die Option *Berechtigungen via LDAP* ist nur verfügbar, wenn LDAP aktiviert ist (siehe Option "LDAP aktiviert" auf Seite 314).

### CAS Benutzer Privileg und Berechtigungen

Mithilfe der Gruppe *CAS Benutzer Privileg und Berechtigungen* können Sie die iRMC S4-Privilegien und -Berechtigungen definieren, die einem Benutzer gewährt werden, wenn er mittels SSO beim iRMC S4 angemeldet ist.

Die Gruppe *CAS Benutzer Privileg und Berechtigungen* wird nicht angezeigt, wenn Sie *Berechtigungen via LDAP* unter *Berechtigungen festlegen von* in der Gruppe *CAS Allgemeine Konfiguration* ausgewählt haben.

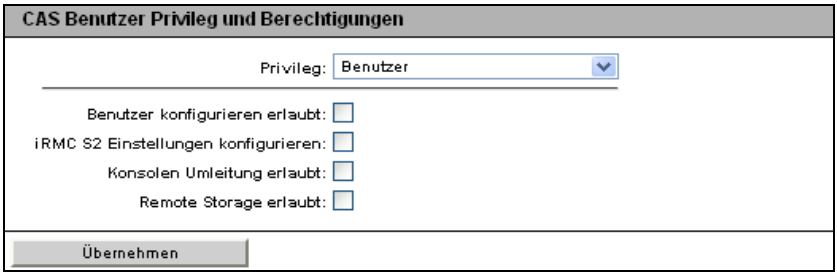



Bild 205: CAS Benutzer Privileg und Berechtigungen

*Berechtigung*

Ordnen Sie hier dem Benutzer eine Berechtigungsgruppe zu:

- *User*
- *Operator*
- *Administrator*
- *OEM*

Zum Berechtigungsumfang der einzelnen Berechtigungsgruppen siehe Abschnitt "Benutzerberechtigungen" auf Seite 65.

Zusätzlich zu den IPMI-spezifischen Berechtigungen können Sie einem Benutzer die folgenden kanalunabhängigen Berechtigungen einzeln erteilen:

*Benutzerkonfiguration erlaubt*

Berechtigung zum Konfigurieren von lokalen Benutzerzugangsdaten.

*iRMC S4-Einstellungen konfigurieren*

Berechtigung zum Konfigurieren der iRMC S4-Einstellungen

*Konsolenumleitung erlaubt*

Berechtigung zur Nutzung der Grafischen Konsolen-Umleitung (Advanced Video Redirection, AVR) im „Nur Lesen“- und „Volle Kontrolle“-Modus.

*Remote Storage erlaubt*

Berechtigung zur Nutzung der Virtual Media-Funktionalität

# 7.16 Konsolen Umleitung - Konsole umleiten

Für die Konsolenumleitung stehen die folgenden Seiten zur Verfügung:

- "BIOS Text Konsole - Textkonsolen-Umleitung konfigurieren und starten" auf Seite 341.
- "Advanced Video Redirection - Advanced Video Redirection (AVR) starten" auf Seite 346.

## 7.16.1 BIOS Text Konsole - Textkonsolen-Umleitung konfigurieren und starten

Über die Seite *BIOS Text Konsole* können Sie die Textkonsolen-Umleitung konfigurieren und starten.

Die Textkonsolen-Umleitung kann auch im BIOS konfiguriert werden (siehe Abschnitt "Text-Konsolen-Umleitung für den iRMC S4 konfigurieren" auf Seite 52).

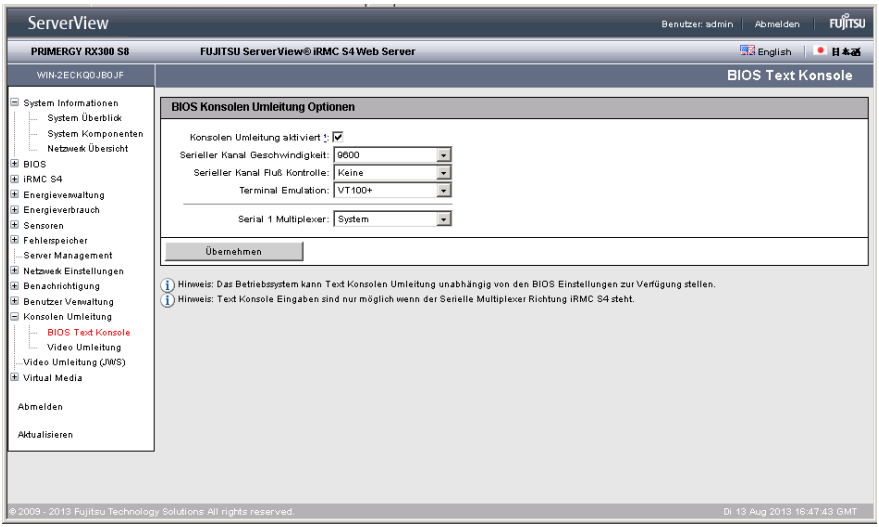



Bild 206: Seite „BIOS Text Konsole“

### 7.16.1.1 BIOS Konsolen Umleitung Optionen - Textkonsolen-Umleitung konfigurieren

Über die *BIOS Konsolen Umleitung Optionen* können Sie die Textkonsolen-Umleitung konfigurieren.

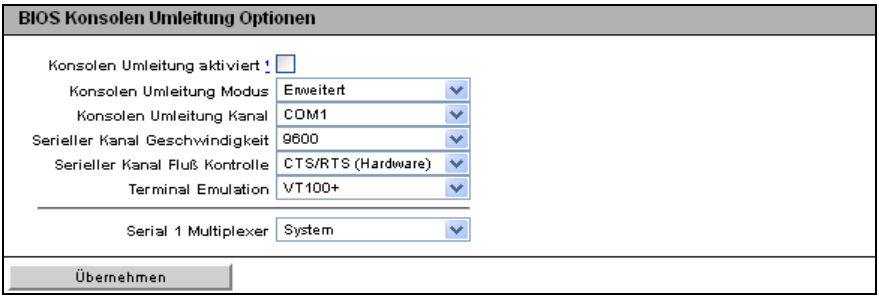



Bild 207: Seite „BIOS Text Konsole“ - BIOS Konsolen Umleitung Optionen

*Konsolen Umleitung aktiviert*

Mit dieser Option können Sie die Konsolenumleitung aktivieren/deaktivieren.

Das Betriebssystem kann auch eine Textkonsolen-Umleitung unabhängig von den Einstellungen im BIOS zulassen.

*Serieller Kanal Geschwindigkeit*

Die folgenden Baud-Raten können festgelegt werden: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

*Serieller Kanal Fluss Kontrolle*

Die folgenden Einstellungen sind möglich:

*Keine*

Die Flusskontrolle ist deaktiviert.

*XON/XOFF (Software)*

Die Flusskontrolle wird von der Software übernommen.

*CTS/RTS (Hardware)*

Die Flusskontrolle wird von der Hardware übernommen.

*Terminal Emulation*

Die folgenden Terminal-Emulationen stehen zur Verfügung:

*VT100 7Bit, VT100 8Bit, PC-ANSI 7Bit, PC-ANSI 8 Bit, VT100+, VT-UTF8*

*Serial 1 Multiplexer*

Überprüfen Sie die Konsistenz der Multiplexer-Einstellungen:

- Seriell: System
- LAN: iRMC S4

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### 7.16.1.2 Textkonsolen-Umleitung bei laufendem Betriebssystem nutzen

Sie können je nach Betriebssystem des verwalteten Servers auch nach der BIOS/UEFI POST-Phase noch die Konsolen-Umleitung nutzen.

#### DOS

Bedingung:

Die BIOS-Einstellung für den Modus der Konsolen-Umleitung muss auf *Erweitert* konfiguriert sein (siehe Abschnitt "BIOS Text Konsole - Textkonsolen-Umleitung konfigurieren und starten" auf Seite 341):

Wenn der verwaltete Server die PRIMERGY ServerView Suite-Diagnosesoftware ausführt, können Sie die PRIMERGY ServerView Suite-Diagnose mithilfe der Konsolen-Umleitung verwenden.

#### Windows Server 2008 / 2012

Windows Server 2008/2012 verarbeitet die Konsolen-Umleitung nach der POST-Phase automatisch. Weitere Einstellungen sind nicht notwendig. Während der Boot-Phase des Betriebssystems wird die SAC-Konsole von Windows Server 2008 oder Windows Server 2012 übertragen:

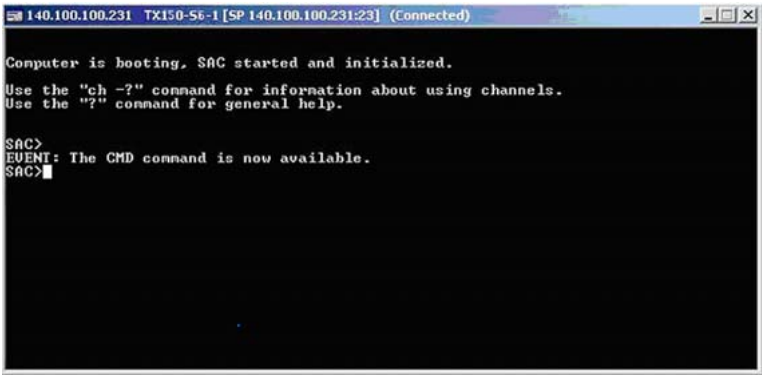

140.100.100.231 TX150-S6-1 [SP 140.100.100.231:23] (Connected)
Computer is booting, SAC started and initialized.
Use the "ch -?" command for information about using channels.
Use the "?" command for general help.
SAC>
EVENT: The CMD command is now available.
SAC>

Bild 208: SAC-Konsole von Windows Server

#### Linux

Ein Linux-Betriebssystem müssen Sie konfigurieren, damit es die Konsolen-Umleitung nach der POST-Phase übernimmt. Nach der Konfiguration haben Sie vollständigen Remote-Zugriff.

### Notwendige Einstellungen

Die Einstellungen können sich je nach Programmversion etwas ändern.

*SuSe und RedHat*

Fügen Sie am Ende der Datei */etc/inittab*: folgende Zeile an

```
xx:12345:respawn:/sbin/agetty <baud-rate> ttyS0
```

*RedHat*

Fügen Sie in die Datei */etc/grub.conf* folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baud-rate> console=tty0
```

*SuSE*

Fügen Sie in die Datei */boot/grub/menu.lst* den folgenden Kernel-Boot-Parameter ein:

```
console=ttyS0,<baud-rate> console=tty0
```

## 7.16.2 Advanced Video Redirection - Advanced Video Redirection (AVR) starten

Über die Seite *Advanced Video Redirection* können Sie die grafische Konsolenumleitung starten. Mit der Funktion „Advanced Video Redirection“ wird die grafische Ausgabe vom verwalteten Server an die Remote-Workstation umgeleitet und die Tastatur- und Mauseingabe von der Remote-Workstation dem verwalteten Server zugewiesen, sodass Sie von der Remote-Workstation aus auf den verwalteten Server zugreifen können, ganz so als würden Sie lokal arbeiten.

AVR kann von zwei Benutzern gleichzeitig verwendet werden. Dabei hat einer der Benutzer die volle Kontrolle über den Server („Volle Kontrolle“-Modus), während der andere Benutzer die Bedienung des Servers via Tastatur- und Mauseingaben nur passiv verfolgen kann („Nur Lesen“-Modus).

Um die iRMC S4-Funktion *Advanced Video Redirection* zu verwenden, benötigen Sie einen Lizenzschlüssel (siehe Abschnitt "iRMC S4 Informationen – Informationen zum iRMC S4" auf Seite 191).

Die AVR-Funktionalität wird über ein Java-Applet zur Verfügung gestellt.

**Wichtiger Hinweis:**

Java Caching **darf nicht** ausgeschaltet sein. Andernfalls kann AVR nicht gestartet werden. (Java Caching ist standardmäßig eingeschaltet).

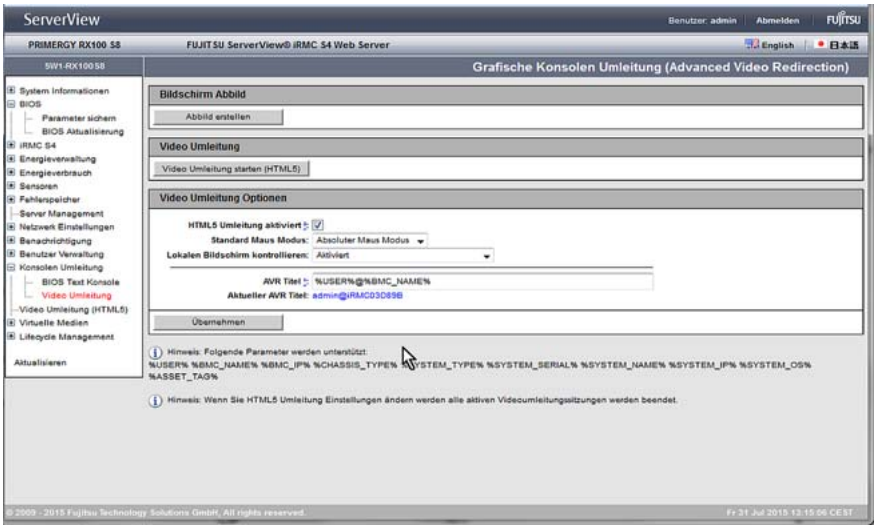



Bild 209: Seite Advanced Video Redirection

### Bildschirm-Abbild erstellen

Über die Seite *Bildschirm Abbild* können Sie

– einen Screenshot des aktuellen VGA-Bildschirms auf dem verwalteten Server (Video-Screenshot) machen und in der Firmware des iRMC S4 speichern,

– den in der iRMC S4-Firmware gespeicherten Screenshot anzeigen,

– den in der iRMC S4-Firmware gespeicherten Screenshot löschen.

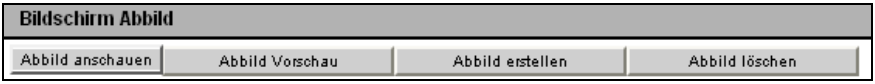



Bild 210: Video-Screenshot erstellen

Bei einem SEL-Eintrag für einen "kritischen Betriebssystemstopp" wird automatisch ein Video-Screenshot erstellt.

In der Firmware des iRMC S4 wird maximal **ein** Video-Screenshot gespeichert, nämlich der zuletzt erstellte Screenshot.

Die folgenden Aktionen sind verfügbar, wenn Sie auf eine der angezeigten Schaltflächen klicken:

*Abbild anschauen*
(Dies wird nur angezeigt, wenn ein Video-Screenshot gespeichert wurde.)
Der Screenshot wird in einem eigenen Browserfenster angezeigt.

*Abbild Vorschau*
(Dies wird nur angezeigt, wenn ein Video-Screenshot gespeichert wurde.)
In der Gruppe *ASR Screenshot* wird eine Miniaturansicht des Screenshots gezeigt.

*Abbild erstellen*
Es wird ein neuer Video-Screenshot aufgenommen.

*Abbild löschen*
(Dies wird nur angezeigt, wenn ein Video-Screenshot gespeichert wurde.)
Der in der iRCM S4-Firmware gespeicherte Video-Screenshot wird gelöscht, sobald Sie diesen Vorgang bestätigt haben.

### Active Konsole Umleitungs Sitzungen - Aktuelle AVR-Sitzungen anzeigen

Die *Active Konsole Umleitungs Sitzungen* enthält die derzeit aktiven AVR-Sitzungen. Wenn derzeit keine AVR-Sitzung aktiv ist, wird die *Active Konsole Umleitungs Sitzungen* nicht angezeigt.

Wenn derzeit zwei AVR-Sitzungen aktiv sind, wird eine Schaltfläche *Trennen* für jede Sitzung angezeigt.

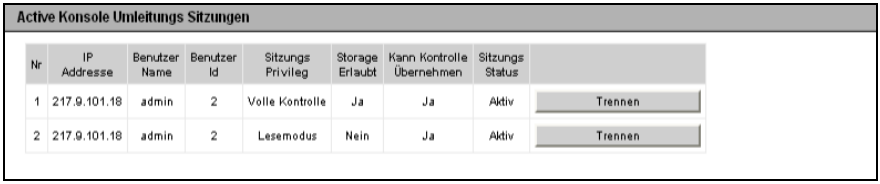



Bild 211: Active Konsole Umleitungs Sitzungen - zwei aktive AVR-Sitzungen

*Trennen*

Wenn Sie auf *Trennen* klicken, wird ein Bestätigungsdialogfenster angezeigt, über das Sie die AVR-Sitzung links von der Schaltfläche schließen können.

Mit der Schaltfläche *Trennen* können Sie nur AVR-Sitzungen von anderen Benutzern schließen. Wählen Sie im AVR-Fenster aus dem Menü *Video* die Option *Beenden* (siehe Seite 98).

### Video Umleitung Optionen

Diese Option wird nicht für alle PRIMERGY Server unterstützt.

Über die Gruppe *Video Umleitung Optionen* können Sie die verschiedenen Optionen festlegen, die für die Dauer der AVR-Sitzung gelten.

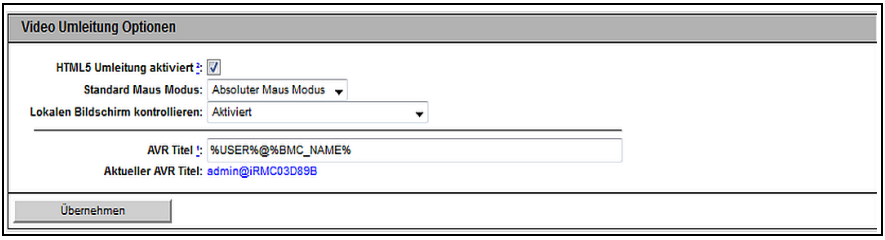



Bild 212: Video Umleitung Optionen

*HTML5 Umleitung aktiviert*

Wenn diese Option aktiviert ist:

- Die Schaltfläche in der Gruppe *Video Umleitung* ändert sich von *Video Umleitung starten (Java Web-Start)* in *Video Umleitung starten (HTML5)*.
- Der Knoten *Video Umleitung (JWS)* im Navigationsbereich ändert sich in *Video Umleitung (HTML5)*.

Beide Elemente öffnen ein Fenster im Browser, das die AVR via HTML5-Oberfläche enthält.

*Standard Maus Mode*

Über diese Option können Sie den Standard-Maus-Modus definieren (*Absoluter Maus-Modus*, *Relativer Maus-Modus* oder *Sonstigen Maus-Modus*).

Je nach Betriebssystem des Servers sind folgende Einstellungen erforderlich:

- Windows: *Absoluter Maus-Modus*, *Lokale Maus verbergen (Relativ)* oder *Relativer Maus-Modus*
- Linux: *Absoluter Maus-Modus*, *Lokale Maus verbergen (Relativ)* oder *Relativer Maus-Modus*

Standardeinstellung: *Absoluter Maus-Modus*

*Lokalen Bildschirm kontrollieren*

Der aktuelle Status des lokalen Monitors wird im AVR-Menü *Video* und über das zweite Symbol von rechts in der AVR-Symbolleiste angezeigt (siehe Abschnitt "AVR-Symbolleiste" auf Seite 118).

Aktiviert/deaktiviert die Funktion *Lokalen Bildschirm kontrollieren* des iRMC S4.

*Aktiviert*

Aktiviert die Funktion *Lokalen Bildschirm kontrollieren*. Im Vollzugriff-Modus einer AVR-Sitzung können Sie den lokalen Bildschirm des Servers von der Remote-Workstation aus ein- und ausschalten:

*Deaktiviert*

Deaktiviert die Funktion *Lokalen Bildschirm kontrollieren*, d. h. der lokale Bildschirm ist dauerhaft eingeschaltet und kann nicht abgeschaltet werden.

*Automatic Off when AVR is started*

Diese Option ist nur verfügbar, wenn *Lokalen Bildschirm kontrollieren* aktiviert ist.

Wenn Sie die Option *Automatic Off when AVR is started* aktivieren, wird der lokale Bildschirm automatisch für die Dauer der Sitzung beim Start einer AVR-Sitzung abgeschaltet. Nachdem die AVR-Sitzung geschlossen wurde, wird der lokale Bildschirm automatisch wieder angeschaltet, wenn nicht gleichzeitig eine Sitzung mit aktivierter Option *Lokalen Bildschirm kontrollieren* aktiv ist.

**Parallele AVR-Sitzungen**:

Selbst wenn Sie den lokalen Bildschirm während Ihrer AVR-Sitzung anschalten, wird er automatisch wieder abgeschaltet, wenn eine neue, gleichzeitige AVR-Sitzung gestartet wird.

Der lokale Bildschirm wird erneut automatisch eingeschaltet, wenn alle AVR-Sitzungen geschlossen wurden.

*AVR Titel*

Titel Ihrer Wahl, der in der AVR-Titelleiste angezeigt wird.

Für den AVR-Titel können Sie die folgenden vordefinierten Variablen verwenden:

```
%USER%, %BMC,_NAME%, %BMC_IP%, %CHASSIS_TYPE%,
%SYSTEM_TYPE%, %SYSTEM_SERIAL%, %SYSTEM_NAME%,
%SYSTEM_IP%, %SYSTEM_OS%, %ASSET_TAG%
```

*Aktueller AVR Titel*

Zeigt den AVR-Titel an, der in der AVR-Titelleiste angezeigt wird.

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

### Video Umleitung - AVR mit Java starten

Die AVR starten Sie unter *Video Umleitung*.

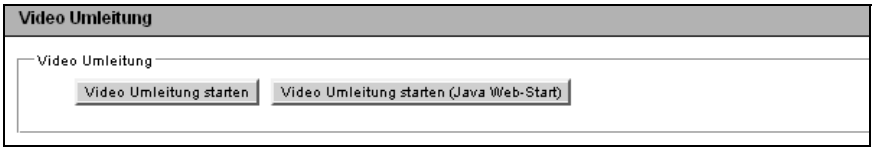



Bild 213: Seite „Advanced Video Redirection“ - Lokaler Bildschirm

► Klicken Sie auf *Video-Umleitung starten (Java Web-Start)*, um eine zweite AVR-Sitzung zu starten.

Das Java-Applet für die Grafische Konsolen-Umleitung wird gestartet.

Einzelheiten zum AVR-Fenster finden Sie unter Kapitel "Advanced Video Redirection (AVR)" auf Seite 83.

Die beiden aktiven AVR-Sitzungen werden wie folgt auf der Seite *Grafische Konsolen Umleitung (AVR)* angezeigt:

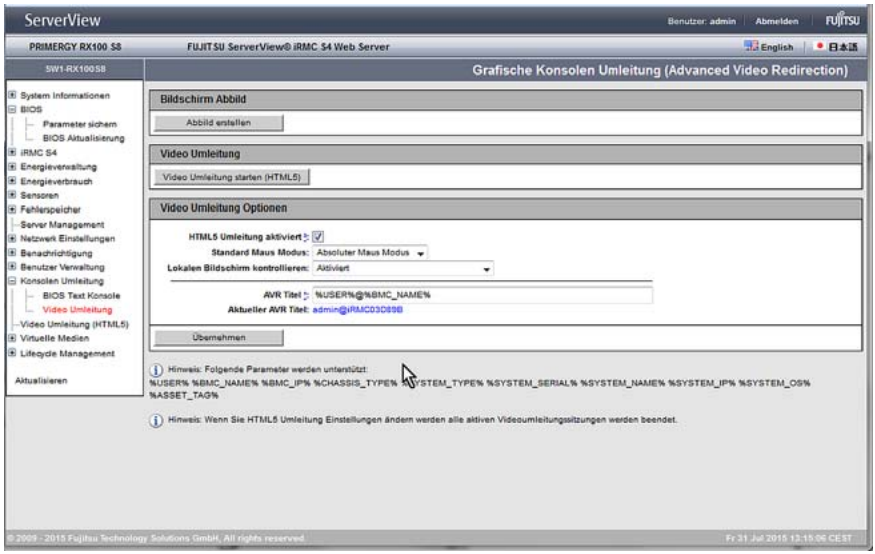



Bild 214: AVR-Fenster mit zwei aktiven AVR-Sitzungen

*Trennen*

Wenn Sie auf *Trennen* klicken, wird ein Bestätigungsdialogfenster angezeigt, über das Sie die AVR-Sitzung links von der Schaltfläche schließen können.

Mit der Schaltfläche *Trennen* können Sie nur AVR-Sitzungen von anderen Benutzern schließen. Wählen Sie im AVR-Fenster aus dem Menü *Video* die Option *Beenden* (siehe Seite 98).

Das folgende Fenster wird angezeigt, wenn der verwaltete Server abgeschaltet ist:

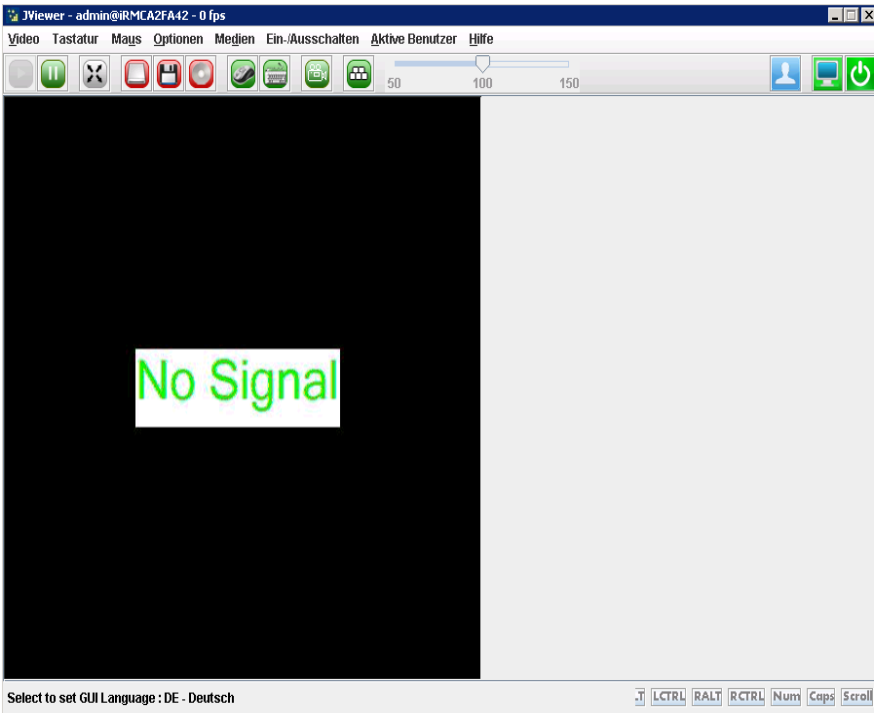

JViewer - admin@iRMCA2FA42 - 0 fps
Video Tastatur Maus Optionen Medien Ein-/Ausschalten Aktive Benutzer Hilfe
50 100 150
No Signal
Select to set GUI Language : DE - Deutsch
LCTRL RALT RCTRL Num Caps Scroll

Bild 215: AVR-Fenster bei abgeschaltetem Server

### Video Umleitung - AVR mit HTML5 starten

Die AVR starten Sie unter *Video Umleitung*.

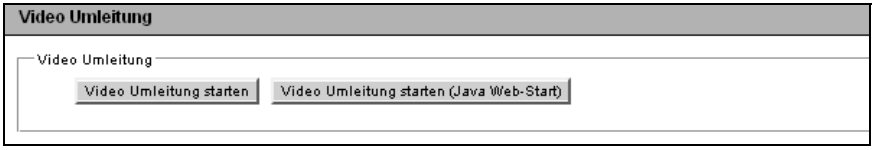



Bild 216: Seite „Advanced Video Redirection“ - Video-Umleitung starten

► Klicken Sie auf *Video-Umleitung starten (HTML5*, um eine zweite AVR-Sitzung zu starten.

Der Standard-Browser startet mit der AVR, siehe Kapitel "Advanced Video Redirection (AVR)" auf Seite 121.

Die aktive Sitzung wird in der Gruppe *AVR Active Sessions Table* angezeigt.

# 7.17 Virtual Media

Mithilfe der Funktion „Virtual Media“ erhält der verwaltete Server ein „virtuelles“ Laufwerk, das sich physikalisch an einer anderen Stelle im Netzwerk befindet. Die Quelle für das virtuelle Laufwerk kann ein physikalisches Laufwerk (Diskette, Festplattenlaufwerk, CD-ROM/DVD-ROM) oder ein ISO-Image (Image-File) sein.

Um die iRMC S4-Funktion *Virtual Media* zu verwenden, benötigen Sie einen Lizenzschlüssel (siehe Seite 193).

Sie können die virtuellen Medien als physikalisches Laufwerk oder als Image-File auf der Remote-Workstation zur Verfügung stellen (siehe Seite 125). Das Image-File kann außerdem ein Netzlaufwerk sein (mit Laufwerksbuchstaben, z. B. „D:“ für Laufwerk D).

Der *Virtual Media*-Link enthält Links zu den folgenden Seiten:

– "Virtual Media Optionen - Virtuelle Medien-Optionen konfigurieren" auf Seite 357.

– "Dezentrale Medien - Remote-ISO-Images verbinden" auf Seite 359.

Dieser Link wird nur angezeigt, wenn die Option *Dezentrale Medien aktiviert* auf der Seite *Virtual Media* aktiviert wurde.

## 7.17.1 Virtual Media Optionen - Virtuelle Medien-Optionen konfigurieren

Über die Seite *Virtual Media Optionen* können Sie die Optionen für die über den iRMC S4 bereitgestellten virtuellen Medien konfigurieren.

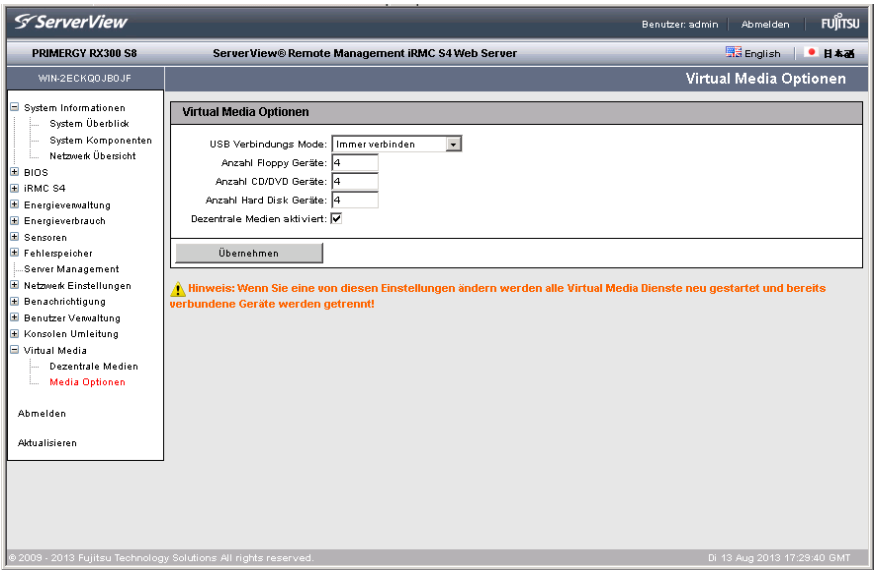


Bild 217: Seite "Virtual Media Optionen"

*USB Verbindungs Mode*
: Verbindungsmodus der virtuellen Medien.

  Die folgenden Modi stehen zur Auswahl bereit:

  *Immer verbinden*
  : Die virtuellen Medien werden immer mit dem Server verbunden.

  *Auto Attach*
  : Die virtuellen Medien werden nur mit dem Server verbunden, wenn eine virtuelle Medien-Sitzung gestartet wird.

*Anzahl Floppy Geräte*
: Maximale Anzahl an Diskettengeräten, die in einer virtuellen Medien-Sitzung verwendet werden können. Es können zwischen 0 und 4 Diskettengeräten konfiguriert werden. Standard: 0.

*Anzahl CD/DVD Geräte*

Maximale Anzahl an CD/DVD-Geräten, die in einer virtuellen Medien-Sitzung verwendet werden können. Es können zwischen 0 und 4 CD/DVD-Geräten konfiguriert werden. Standard: 2.

*Anzahl Hard Disk Geräte*

Maximale Anzahl an Festplatten-Geräten, die in einer virtuellen Medien-Sitzung verwendet werden können. Es können zwischen 0 und 4 Festplatten-Geräten konfiguriert werden. Standard: 1.

*Dezentrale Medien aktiviert*

Aktiviert/deaktiviert dezentrale Medien, sodass Sie CD/DVD-, Disketten- und Festplatten-ISO-Images auf einem Server im Netzwerk hosten können.

Durch Aktivieren der Option „*Dezentrale Medien aktiviert*“ wird der zusätzliche Link *Dezentrale Medien* unter *Virtual Media* im Navigationsbereich angezeigt. Durch Klicken auf den Link *Dezentrale Medien* wird die Seite *Dezentrale Medien* angezeigt, die Bedienfelder für die Konfiguration der *Optionen für dezentrale Abbilder* der entsprechenden Image-Typen enthält (siehe Seite 359).

► Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.

## 7.17.2 Dezentrale Medien - Remote-ISO-Images verbinden

Die Funktion „Dezentrale Medien“ stellt dem verwalteten Server CD/DVD-, Disketten- und Festplatten-ISO-Images zur Verfügung, auf denen ein Server im Netzwerk gehostet wird.

Die Seite *Dezentrale Medien* enthält Gruppen zum Konfigurieren der *Optionen für die dezentralen Abbilder* des entsprechenden Image-Typs (CD/DVD, Diskette und Festplatten-ISO-Images).

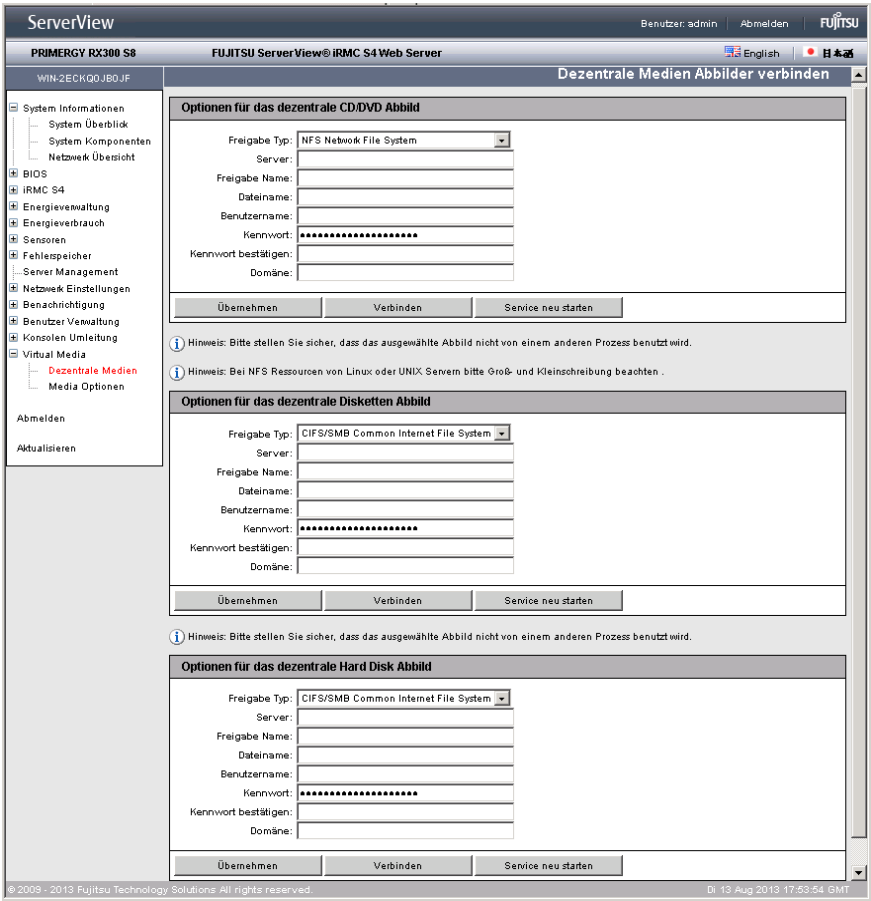



Bild 218: Seite „Dezentrale Medien“

### Optionen für das dezentrale CD/DVD Abbild / Optionen für das dezentrale Disketten Abbild / Optionen für das dezentrale Hard Disk Abbild

Mit diesen Gruppen können Sie jeweils die Optionen für das Verbinden von Remote-Images des entsprechenden Typs konfigurieren und die Verbindung des Remote-Images herstellen bzw. löschen. Darüber hinaus können Sie den Service *Dezentrale Medien* neu starten (z. B. im Fall eines Ausfalls).

*Freigabe Typ*
: Der Freigabetyp des Netzlaufwerks, auf dem sich die ISO-Images befinden.

  Die folgenden Modi stehen zur Auswahl bereit:

  *CIFS/SMB Common Interface File System*
  : Der Freigabetyp des Netzlaufwerks lautet „CIFS SMB (Common Interface File System)“.

  *NFS Network File System*
  : Die virtuellen Medien werden nur mit dem Server verbunden, wenn eine virtuelle Medien-Sitzung gestartet wird.

*Server*
: IP-Adresse oder DNS-Name des Servers, auf dem die Remote-Images gehostet werden (der Remote-Image-Server).

*Freigabe Name*
: Name des Netzlaufwerks, zu dem der Remote-Image-Server gehört.

*Dateiname*
: Name/Pfad des Remote-Images.

*Benutzername*
: Benutzername, der für den Zugriff auf das Netzlaufwerk erforderlich ist.

*Kennwort*
: Tragen Sie hier das Kennwort des Benutzers ein.

*Kennwort bestätigen*
: Wiederholen Sie zur Bestätigung die Eingabe des Kennworts.

*Domäne*
: Domäne des Benutzers.

*Übernehmen*
: Aktiviert Ihre Einstellungen

*Verbinden*
: Verbindet das Remote-Image mit dem verwalteten Server.

*Trennen*
Löscht die Verbindung des Remote-Images.

*Service neu starten*
Startet den Dienst „Dezentrale Medien“ (z. B. im Fall eines Ausfalls).

### Remote-Image mit dem verwalteten Server verbinden

Bei der folgenden Konfiguration der *Optionen für das dezentrale CD/DVD Abbild*:

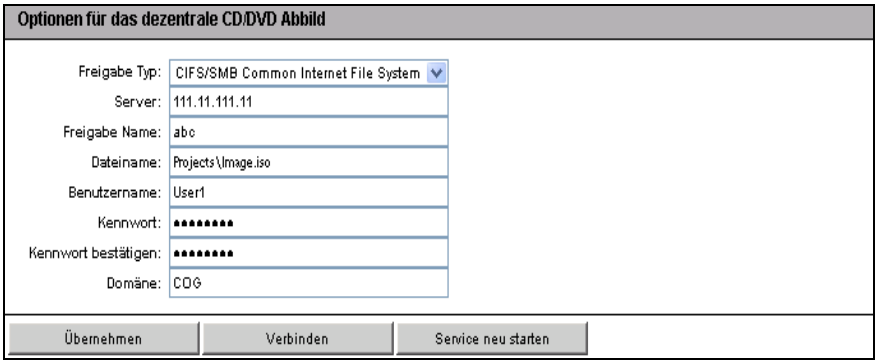



Bild 219: Konfigurierte Optionen für das dezentrale CD/DVD Abbild

Gehen Sie folgendermaßen vor, um das Remote-Image mit dem verwalteten Server zu verbinden:

- Klicken Sie auf *Übernehmen*, um Ihre Einstellungen zu aktivieren.
- Klicken Sie auf *Verbinden*.

  Die Gruppe *Optionen für das dezentrale CD/DVD Abbild* wird folgendermaßen angezeigt und gibt an, dass das Remote-Image jetzt mit dem verwalteten Server verbunden ist:

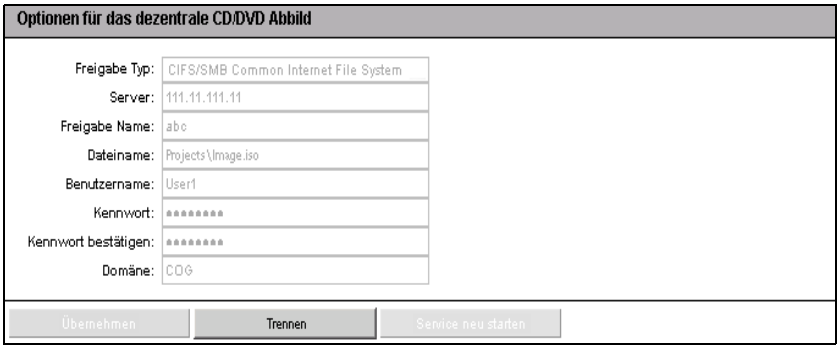



Bild 220: Optionen für das dezentrale CD/DVD Abbild

- Klicken Sie auf *Trennen*, um die Verbindung mit dem Remote-Image zu löschen.
- Um den Dienst *Dezentrale Medien* (z. B. im Fall eines Ausfalls) neu zu starten, klicken Sie auf *Service neu starten*.

# 7.18 Lifecycle Management

Die eLCM-Funktion (embedded Lifecycle Management) des iRMC S4 ermöglicht es Ihnen, die Lebenszyklusverwaltung von PRIMERGY Servern mit wenigen Mausklicks zentral über die iRMC S4-Weboberfläche zu konfigurieren und auszuführen, ohne dass hierfür physische Geräte eingesetzt werden müssen.

Die vom iRMC S4 bereitgestellte eLCM-Lösung beinhaltet die folgenden Funktionen:

– eLCM Update Management

– eLCM Image Management

– eLCM Health Management

Für die Verwendung der eLCM-Funktion ist ein gültiger eLCM-Lizenzschlüssel erforderlich, der zusammen mit der SD-Karte des iRMC S4 gekauft wird. Die SD-Karte wird als nicht flüchtiger Massenspeicher des iRMC S4 verwendet und im internen Linux-Dateisystem des iRMC S4 gemountet. Auf der Serverseite können Dateien auf der SD-Karte des iRMC S4 über die PCIe-Schnittstelle per HTI (High-speed Transfer Protocol) gelesen und geschrieben werden. Insbesondere die Kommunikation zwischen dem iRMC S4 und dem ServerView Agentless Service erfolgt per HTI.

Der Link *Lifecycle Management* enthält Links auf die folgenden Seiten:

– "Aktualisierungs Einstellungen – allgemeine eLCM-Update-Einstellungen konfigurieren" auf Seite 365.

– "Online Aktualisierung – eLCM-Online-Aktualisierung konfigurieren" auf Seite 366.

– "Offline Aktualisierung – eLCM-Offline-Aktualisierung konfigurieren" auf Seite 372.

– "Custom Image – benutzerdefinierte Images verwenden" auf Seite 378.

– "PrimeCollect – Health Management" auf Seite 383.

Der iRMC S4 unterstützt eine SD-Karte für den nicht flüchtigen Massenspeicher. Die SD-Karte wird im internen Linux-Dateisystem des iRMC S4 gemountet. Auf der Serverseite können Dateien auf der SD-Karte des iRMC S4 über die PCIe-Schnittstelle per HTI gelesen und geschrieben werden.

Für die Verwendung der iRMC S4-Funktion *Lifecycle Management* ist ein Lizenzschlüssel erforderlich (siehe Seite 193).

## 7.18.1 Aktualisierungs Einstellungen – allgemeine eLCM-Update-Einstellungen konfigurieren

Auf der Seite *Aktualisierungs Einstellungen* können Sie die Optionen für das eLCM-Update-Repository konfigurieren.

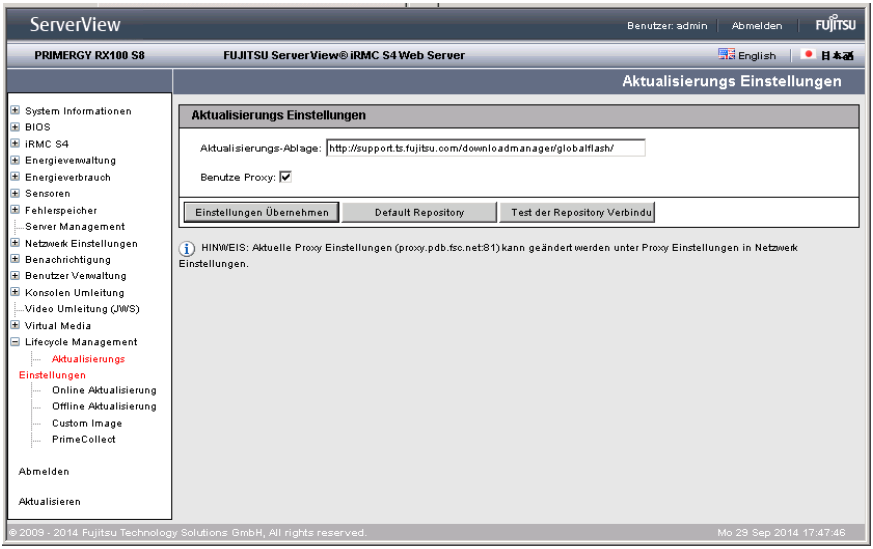



Bild 221: Seite "Allgemeine Aktualisierungs Einstellungen"

*Aktualisierungs-Ablage*

URL des für das eLCM-Update verwendeten Update-Repositorys. Standard: *https://support.ts.fujitsu.com*

*Benutze Proxy*

Legt fest, ob ein Proxyserver verwendet werden soll. Die Proxyeinstellungen können auf der Seite *Netzwerk Einstellungen – Proxy Einstellungen* konfiguriert/geändert werden (siehe Seite 280).

*Einstellungen Übernehmen*

Wendet die Einstellungen an.

*Default Repository*

Der Repository-Ort ist auf die Standardeinstellung gesetzt (*https://support.ts.fujitsu.com*).

*Test der Repository Verbindung*

Testet die Verbindung zum Repository.

## 7.18.2 Online Aktualisierung – eLCM-Online-Aktualisierung konfigurieren

Auf der Seite *Online Aktualisierung* können Sie BIOS- und Controller-Firmware aktualisieren, während das Serverbetriebssystem ausgeführt wird. Bei Windows-Systemen können auch von PSPs (PRIMERGY Support Packages, weitere Einzelheiten siehe Handbuch "Lokaler System Update von PRIMERGY Servern") unterstützte Treiber aktualisiert werden.

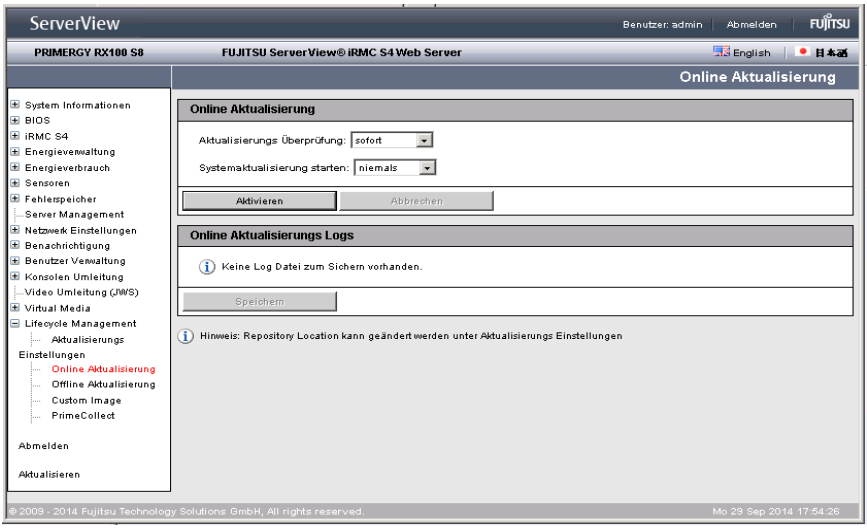



Bild 222: Seite "Online Aktualisierung"

Der Start einer Online-Aktualisierung beinhaltet immer die folgenden Schritte:

1. Aktualisierungsüberprüfung durchführen.
2. Online-Aktualisierungsvorgang starten.

Beide Schritte, die nachfolgend genauer beschrieben werden, können manuell oder geplant ausgeführt werden.

Die vollständige Online-Aktualisierungsfunktion ist nur verfügbar, wenn der ServerView Agentless Service auf dem Serverbetriebssystem ausgeführt wird. Andernfalls kann nur iRMC S4- und/oder BIOS-Firmware aktualisiert werden. In der Gruppe *System Informationen* auf der Seite *System Überblick* wird angezeigt, ob der ServerView Agentless Service verfügbar ist (siehe Seite 151).

Der ServerView Agentless Service stellt Inventory-Daten für Treiber und Firmware bereit und installiert die Komponententreiber- und Firmware-Aktualisierungen auf dem verwalteten Server, während das System ausgeführt wird.

Eine genauere Beschreibung hierzu erhalten Sie im Handbuch "ServerView embedded Lifecycle Management (eLCM)".

### Online Aktualisierung – Online-Aktualisierung konfigurieren und starten

In der Gruppe *Online Aktualisierung* können Sie sowohl die Aktualisierungsüberprüfung als auch die Online-Aktualisierung selbst konfigurieren und starten.

Die Aktualisierungseinstellungen können nicht geändert werden, während eine Aktualisierung ausgeführt wird.

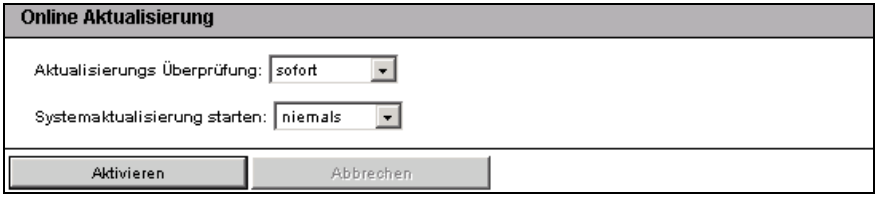



Bild 223: Seite "Online Aktualisierung" – Gruppe "Online Aktualisierung"

*Aktualisierungs Überprüfung*

Hier können Sie konfigurieren, ob durch die Auswahl von *Aktivieren* die Aktualisierungsüberprüfung sofort, an einem bestimmten Datum oder in regelmäßigen Abständen gestartet wird.

*sofort*

Startet die Aktualisierungsüberprüfung sofort.

*täglich*

Startet die Aktualisierungsüberprüfung einmal pro Tag zur festgelegten Uhrzeit.

*wöchentlich*

Startet die Aktualisierungsüberprüfung einmal pro Woche am festgelegten Tag und zur festgelegten Uhrzeit.

*monatlich*

Startet die Aktualisierungsüberprüfung einmal pro Monat am festgelegten Tag und zur festgelegten Uhrzeit.

*jährlich*

Startet die Aktualisierungsüberprüfung einmal pro Jahr am festgelegten Datum und zur festgelegten Uhrzeit.

*nur einmal*

Startet die Aktualisierungsüberprüfung am festgelegten Datum und zur festgelegten Uhrzeit.

*niemals*

Führt niemals eine Aktualisierungsüberprüfung durch.

Nachdem der Vorgang der Aktualisierungsüberprüfung erfolgreich abgeschlossen wurde, wird in der Gruppe *Online Aktualisierung* die Liste *Verfügbare Aktualisierungen* angezeigt. Dort können Sie die zu aktualisierenden Komponenten auswählen bzw. deren Auswahl aufheben.

Die Auswahl von Aktualisierungen, für die bei *Dringlichkeit* die Gewichtung "essential" angezeigt wird, kann nicht aufgehoben werden.

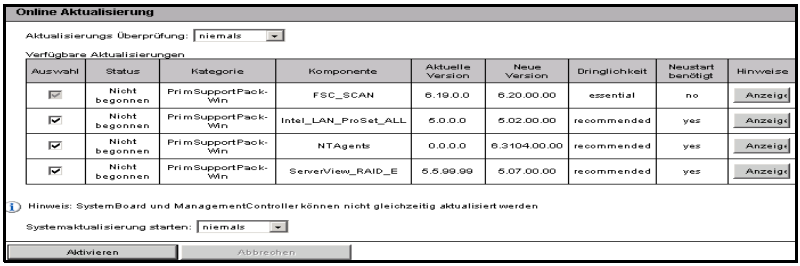



Bild 224: Gruppe "Online Aktualisierung" – Aktualisierungsüberprüfung durchgeführt

*Systemaktualisierung starten*

Hier können Sie konfigurieren, ob durch die Auswahl von *Aktivieren* der Aktualisierungsvorgang sofort, an einem bestimmten Datum oder in regelmäßigen Abständen gestartet wird.

*sofort*

Startet den Aktualisierungsvorgang sofort.

*nach Überprüfung*

Startet automatisch einen Aktualisierungsvorgang, der direkt auf eine (sofort) gestartete Aktualisierungsüberprüfung folgt.

*täglich*
: Startet den Aktualisierungsvorgang einmal pro Tag zur festgelegten Uhrzeit.

*wöchentlich*
: Startet den Aktualisierungsvorgang einmal pro Woche am festgelegten Tag und zur festgelegten Uhrzeit.

*monatlich*
: Startet den Aktualisierungsvorgang einmal pro Monat am festgelegten Tag und zur festgelegten Uhrzeit.

*jährlich*
: Startet den Aktualisierungsvorgang einmal pro Jahr am festgelegten Datum und zur festgelegten Uhrzeit.

*nur einmal*
: Startet den Aktualisierungsvorgang am festgelegten Datum und zur festgelegten Uhrzeit.

*niemals*
: Führt niemals einen Aktualisierungsvorgang durch.

*Aktivieren*
: Startet eine Aktualisierungsüberprüfung und/oder die Online-Aktualisierung gemäß den Einstellungen, die unter *Aktualisierungs Überprüfung* und *Systemaktualisierung starten* konfiguriert sind:

| **Aktualisierungs Überprüfung** | **Systemaktualisierung starten** | **Verhalten** |
|---|---|---|
| sofort | nach Überprüfung | Die Aktualisierungsüberprüfung wird sofort gestartet. Anschließend wird automatisch der Aktualisierungsvorgang gestartet. Alle verfügbaren Aktualisierungskomponenten werden installiert. Kein Benutzereingriff. |
| geplant[1] | nach Überprüfung | Geplante Aktualisierungsüberprüfung. Alle verfügbaren Aktualisierungskomponenten werden installiert. Kein Benutzereingriff. |
| sofort | niemals | Die Aktualisierungsüberprüfung wird sofort gestartet. Der Aktualisierungsvorgang wird nicht automatisch gestartet. |

Tabelle 9: Einstellungen für Online-Aktualisierungen

| Aktualisierungs Überprüfung | Systemaktualisierung starten | Verhalten |
|---|---|---|
| geplant[1] | niemals | Geplante Aktualisierungsüberprüfungen, auf die kein automatisch gestarteter Aktualisierungsvorgang folgt. |
| niemals | sofort | Ausgehend vom Ergebnis einer separat durchgeführten Aktualisierungsüberprüfung wird der Aktualisierungsvorgang sofort gestartet. Dadurch können Sie eine oder mehrere der von der vorhergehenden Aktualisierungsüberprüfung zur Auswahl angebotenen Komponenten ausdrücklich auswählen bzw. deren Auswahl aufheben, bevor der Aktualisierungsvorgang gestartet wird. |
| niemals | geplant[1] | Ausgehend vom Ergebnis einer separat durchgeführten Aktualisierungsüberprüfung wird der Aktualisierungsvorgang sofort gestartet. Dadurch können Sie eine oder mehrere der von der vorhergehenden Aktualisierungsüberprüfung zur Auswahl angebotenen Komponenten ausdrücklich auswählen bzw. deren Auswahl aufheben, bevor der Aktualisierungsvorgang gestartet wird. |

Tabelle 9: Einstellungen für Online-Aktualisierungen

[1] täglich, wöchentlich, monatlich, jährlich, nur einmal

*Abbrechen*

Bricht die Aktualisierungsüberprüfung ab.

### Online Aktualisierungs Logs

In der Gruppe *Online Aktualisierungs Logs* wird angezeigt, ob eine Log-Datei der Online-Aktualisierungen verfügbar ist. Falls dies der Fall ist, können Sie die Log-Datei speichern.

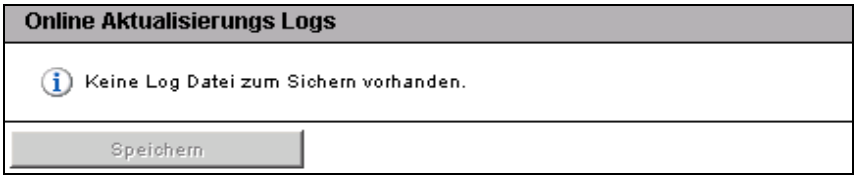



Bild 225: Seite "Online Aktualisierung" – Online Aktualisierungs Logs

*Speichern*

Öffnet ein Bestätigungsdialogfenster, über das die Log-Datei gespeichert werden kann. Die Schaltfläche *Speichern* ist deaktiviert, wenn keine Log-Datei verfügbar ist.

## 7.18.3 Offline Aktualisierung – eLCM-Offline-Aktualisierung konfigurieren

Auf der Seite *Offline Aktualisierung* können Sie Systemkomponenten wie Controller-Firmware für das Netzwerk oder die Speicherung auf dem verwalteten Server aktualisieren. Außerdem können Sie Aktualisierungen für BIOS- und iRMC S4-Firmware installieren.

Eine Offline-Aktualisierung kann verwendet werden, wenn kein Agentless Service auf dem verwalteten Server ausgeführt wird oder wenn der Agentless Service das Serverbetriebssystem nicht unterstützt. In der Gruppe *System Informationen* auf der Seite *System Überblick* wird angezeigt, ob der ServerView Agentless Service auf dem Server verfügbar ist (siehe Seite 151).

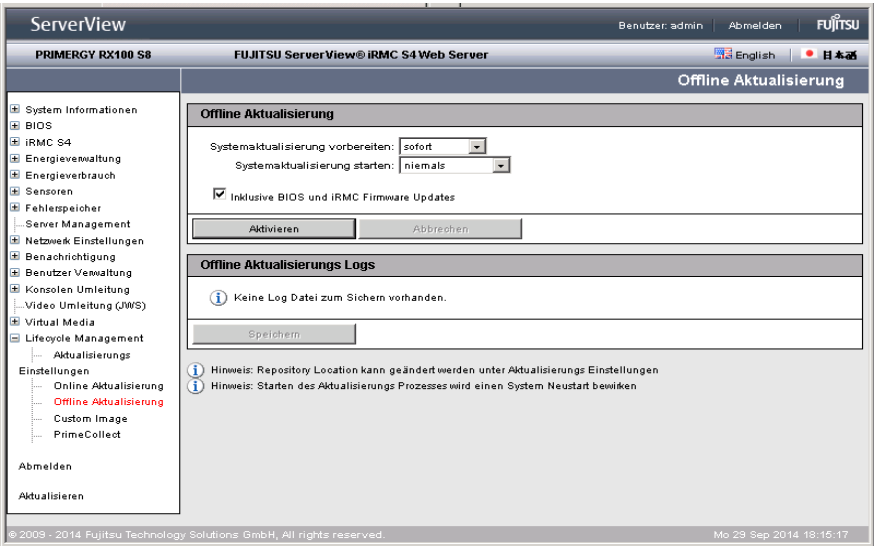


Bild 226: Seite "Offline Aktualisierung"

Die Offline-Aktualisierung beinhaltet in etwa die folgenden Schritte, die automatisch verarbeitet werden:

1. Der iRMC lädt alle erforderlichen Dateien (insbesondere eLCM Offline Update Manager, eine abgespeckte Version von ServerView Update Manager Express) und das lokale Update-Repository auf die SD-Karte des iRMC herunter.

2. Der iRMC erstellt ein bootfähiges CD-ROM-Image von diesen Komponenten und mountet dieses als virtuelles CD-ROM-Gerät.
3. Der iRMC fährt den verwalteten Server herunter und startet das System über das gemountete CD-ROM-Gerät neu.
4. eLCM Offline Update Manager, eine abgespeckte Version von ServerView Update Manager Express, installiert die Firmware-Aktualisierungen.

Eine genauere Beschreibung hierzu erhalten Sie im Handbuch "ServerView embedded Lifecycle Management (eLCM)".

Der Start einer Offline-Aktualisierung beinhaltet immer die folgenden Schritte:

1. Offline-Aktualisierung vorbereiten.
2. Offline-Aktualisierungsvorgang starten.

Beide Schritte, die nachfolgend genauer beschrieben werden, können manuell oder geplant ausgeführt werden.

### Offline Aktualisierung – Offline-Aktualisierung vorbereiten und starten

In der Gruppe *Offline Aktualisierung* können Sie den Offline-Aktualisierungsvorgang vorbereiten und starten.

Die Aktualisierungseinstellungen können nicht geändert werden, während eine Aktualisierung ausgeführt wird.

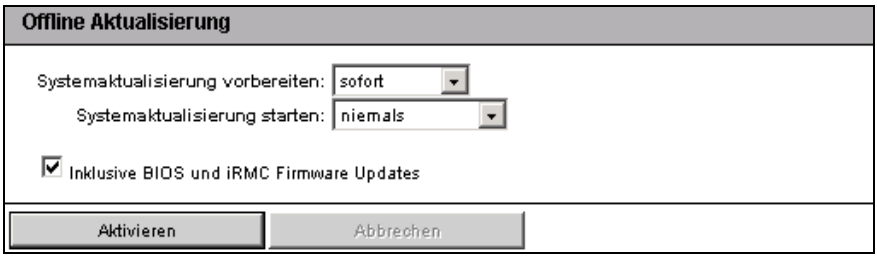



Bild 227: Seite "Offline Aktualisierung" – Gruppe "Offline Aktualisierung"

*Systemaktualisierung vorbereiten*

Bereitet die Offline-Aktualisierung vor.

Die Vorbereitung der Offline-Aktualisierung beinhaltet die folgenden Aktivitäten, die vom iRMC S4 automatisch durchgeführt werden:

- Aktualisierungspakete mit der aktuellen Firmware für Systemkomponenten, iRMC S4-Firmware und das BIOS auf den iRMC S4 herunterladen.
- Systemspezifische lokale Kopie von *Update-DVD.iso* erstellen. Es werden nur Komponenten berücksichtigt, die für den verwalteten Server relevant sind.

Hier können Sie konfigurieren, ob durch die Auswahl von *Aktivieren* die Vorbereitung des Offline-Aktualisierungsvorgang sofort, an einem bestimmten Datum oder in regelmäßigen Abständen gestartet wird.

*sofort*

Bereitet die Aktualisierung sofort vor.

*täglich*

Bereitet die Aktualisierung einmal pro Tag zur festgelegten Uhrzeit vor.

*wöchentlich*

Bereitet die Aktualisierung einmal pro Woche am festgelegten Tag und zur festgelegten Uhrzeit vor.

*monatlich*

Bereitet den Aktualisierungsvorgang einmal pro Monat am festgelegten Tag und zur festgelegten Uhrzeit vor.

*jährlich*

Bereitet die Aktualisierung einmal pro Jahr am festgelegten Datum und zur festgelegten Uhrzeit vor.

*nur einmal*

Bereitet die Aktualisierung am festgelegten Datum und zur festgelegten Uhrzeit vor.

*niemals*

Führt niemals einen Aktualisierungsvorgang durch.

*Systemaktualisierung starten*

Hier können Sie konfigurieren, ob durch die Auswahl von *Aktivieren* die Aktualisierungsüberprüfung sofort, an einem bestimmten Datum oder in regelmäßigen Abständen gestartet wird.

*sofort*

Startet den Aktualisierungsvorgang sofort.

*nach Vorbereitung*

Startet automatisch einen Aktualisierungsvorgang, der direkt auf eine (sofort) gestartete Aktualisierungsvorbereitung folgt.

*täglich*

Startet den Aktualisierungsvorgang einmal pro Tag zur festgelegten Uhrzeit.

*wöchentlich*

Startet den Aktualisierungsvorgang einmal pro Woche am festgelegten Tag und zur festgelegten Uhrzeit.

*monatlich*

Startet den Aktualisierungsvorgang einmal pro Monat am festgelegten Tag und zur festgelegten Uhrzeit.

*jährlich*

Startet den Aktualisierungsvorgang einmal pro Jahr am festgelegten Datum und zur festgelegten Uhrzeit.

*nur einmal*

Startet den Aktualisierungsvorgang am festgelegten Datum und zur festgelegten Uhrzeit.

*niemals*

Führt niemals einen Aktualisierungsvorgang durch.

*Inklusive BIOS und iRMC Firmware Updates*

Diese Option hat Einfluss auf den Vorbereitungsprozess der Offline-Aktualisierung.

Gibt an, ob die Datei UserProfile.xml die BIOS- und iRMC-Firmware-Aufgaben zur Vorbereitung der Offline-Aktualisierung enthält oder nicht enthält. So enthält das ISO-Image immer die Update-Dateien, aber die Update-Aufgaben sind entweder enthalten oder nicht.

*Aktivieren*

Startet eine Aktualisierungsüberprüfung und/oder die Offline-Aktualisierung gemäß den Einstellungen, die unter *Systemaktualisierung vorbereiten* und *Systemaktualisierung starten* konfiguriert sind:

| **Systemaktualisierung vorbereiten** | **Systemaktualisierung starten**[1] | **Verhalten** |
|---|---|---|
| sofort | niemals | Die Vorbereitung der Offline-Aktualisierung wird sofort gestartet. Der Aktualisierungsvorgang wird nicht automatisch gestartet. |
| sofort | nach Vorbereitung | Die Vorbereitung der Offline-Aktualisierung wird sofort gestartet. Anschließend wird automatisch der Aktualisierungsvorgang gestartet. Kein Benutzereingriff. |
| geplant[2] | niemals | Die geplante Vorbereitung der Offline-Aktualisierung wird sofort gestartet. Der Aktualisierungsvorgang wird nicht automatisch gestartet. |
| geplant[2] | auto | Geplante Vorbereitung der Aktualisierung in Verbindung mit anschließend gestartetem Aktualisierungsvorgang. Alle verfügbaren Aktualisierungskomponenten werden installiert. Kein Benutzereingriff. |
| niemals | sofort | Der Aktualisierungsvorgang wird sofort gestartet. Hierzu ist es erforderlich, dass ein von einer vorhergehenden Aktualisierungsvorbereitung bereitgestelltes Aktualisierungs-ISO-Image bereits auf dem iRMC S4 verfügbar ist. |
| niemals | geplant[2] | Der Aktualisierungsvorgang wird geplant gestartet. Hierzu ist es erforderlich, dass ein von einer vorhergehenden Aktualisierungsvorbereitung bereitgestelltes Aktualisierungs-ISO-Image bereits auf dem iRMC S4 verfügbar ist. |

Tabelle 10: Einstellungen für Offline-Aktualisierungen

[1] Nach dem Start des Aktualisierungsvorgangs wird der verwaltete Server heruntergefahren. eLCM Offline Update Manager wird gestartet und führt die Aktualisierung durch.

[2] täglich, wöchentlich, monatlich, jährlich, nur einmal

*Abbrechen*

Bricht die Vorbereitung/Ausführung der Offline-Aktualisierung ab. *Abbrechen* funktioniert nur, solange der Download nicht gestartet wurde. Nach dem Start des Downloads ist die Schaltfläche *Abbrechen* deaktiviert.

### Offline Aktualisierungs Logs

In der Gruppe *Offline Aktualisierungs Logs* wird angezeigt, ob eine Log-Datei in Bezug auf die Offline-Aktualisierung verfügbar ist. Falls dies der Fall ist, können Sie die Log-Datei speichern.

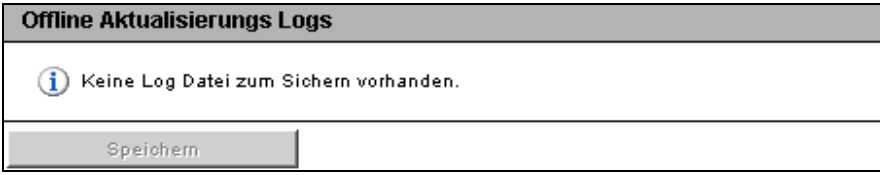



Bild 228: Seite "Online Aktualisierung" – Online Aktualisierungs Logs

*Speichern*

Öffnet ein Bestätigungsdialogfenster, über das die Log-Datei gespeichert werden kann. Die Schaltfläche *Speichern* ist deaktiviert, wenn keine Log-Datei verfügbar ist.

## 7.18.4 Custom Image – benutzerdefinierte Images verwenden

Auf der Seite *Custom Image* können Sie eine URL festlegen, über die Sie ISO-Images auf die SD-Karte des iRMC S4 herunterladen können. Der Download kann manuell gestartet oder über einen Timer geplant werden. Die heruntergeladenen Images werden anschließend zur Auswahl angezeigt.

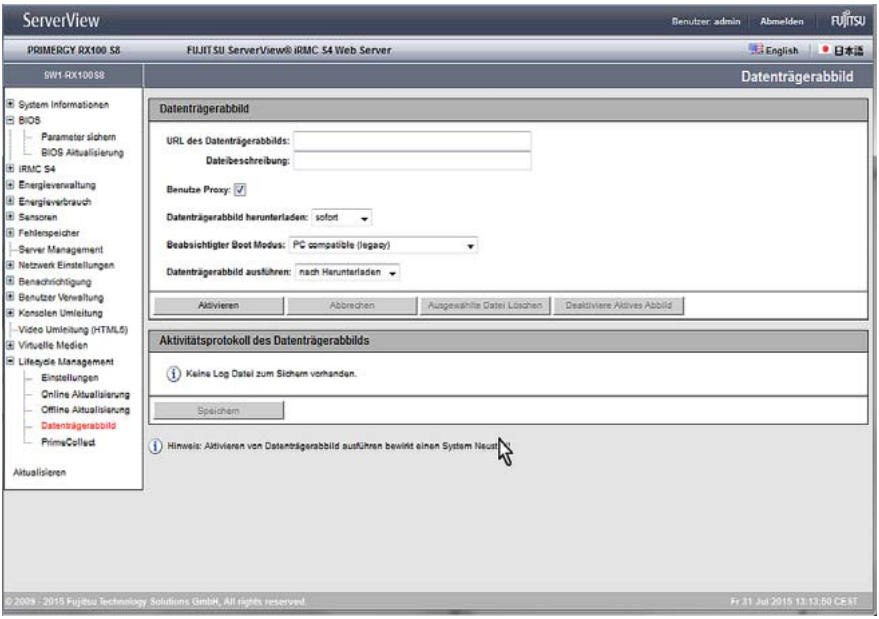


Bild 229: Seite "Custom Image"

*Custom Image URL*

Hier können Sie die URL festlegen, über die ISO-Images auf den iRMC S4 heruntergeladen werden sollen.

*Dateibeschreibung*

Hier können Sie eine Textbeschreibung des Images eingeben.

*Download Custom Image*

Hier können Sie konfigurieren, ob durch die Auswahl von *Aktivieren* der Download des benutzerdefinierten Images sofort, automatisch an einem bestimmten Datum oder in regelmäßigen Abständen gestartet wird.

*sofort*

Lädt das benutzerdefinierte Image sofort herunter.

*nur einmal*

Lädt das benutzerdefinierte Image am festgelegten Datum und zur festgelegten Uhrzeit herunter.

*niemals*

Führt niemals einen Download des benutzerdefinierten Images durch.

*Intended Boot Mode*

Gibt den beabsichtigten ersten Boot-Modus an, der einem neuen heruntergeladenen ISO-Image zugewiesen werden soll. Wenn Sie einen automatisch gesteuerten Boot-Modus ausgewählt haben (z. B. “nach dem Download”, “täglich”, “wöchentlich”), dann wird dieser Boot-Modus verwendet. In der Liste *Downloaded Custom Image* ist eine neue Spalte mit dem Namen Intended Boot Mode.

– PC compatible (legacy)

– Extensible Firmware Interface Boot (EFI)

*Execute Custom Image*

Hier können Sie konfigurieren, ob durch die Auswahl von *Aktivieren* die Ausführung des benutzerdefinierten Images sofort, automatisch an einem bestimmten Datum oder in regelmäßigen Abständen gestartet wird.

*nach Download*

Führt das benutzerdefinierte Image automatisch nach einem (sofort) gestarteten Download aus.

*sofort*

Führt das benutzerdefinierte Image sofort aus.

*täglich*

Führt das benutzerdefinierte Image einmal pro Tag zur festgelegten Uhrzeit aus.

*wöchentlich*

Führt das benutzerdefinierte Image einmal pro Woche am festgelegten Tag und zur festgelegten Uhrzeit aus.

*monatlich*

Führt das benutzerdefinierte Image einmal pro Monat am festgelegten Tag und zur festgelegten Uhrzeit aus.

*jährlich*

Führt das benutzerdefinierte Image einmal pro Jahr am festgelegten Datum und zur festgelegten Uhrzeit aus.

*nur einmal*

Führt das benutzerdefinierte Image am festgelegten Datum und zur festgelegten Uhrzeit aus.

*niemals*

Führt niemals eine Ausführung des benutzerdefinierten Images durch.

*Aktivieren*

Startet den Download und/oder die Ausführung des ausgewählten benutzerdefinierten Images gemäß den Einstellungen, die unter *Download Custom Image* und *Execute Custom Image* konfiguriert sind:

| **Download Custom Image** | **Execute Custom Image** | **Verhalten** |
|---|---|---|
| sofort | niemals | Der Download des benutzerdefinierten Images wird sofort gestartet. Das benutzerdefinierte Image wird nicht automatisch ausgeführt. |
| geplant[1] | niemals | Der geplante Download des benutzerdefinierten Images wird sofort aktiviert. Das benutzerdefinierte Image wird nicht automatisch ausgeführt. |
| sofort | nach Download | Der Download des benutzerdefinierten Images wird sofort gestartet. Anschließend wird automatisch die Ausführung des benutzerdefinierten Images gestartet. Kein Benutzereingriff. |
| geplant[1] | nach Download | Geplanter Download des benutzerdefinierten Images in Verbindung mit einer anschließenden automatisch gestarteten Ausführung. Kein Benutzereingriff. |
| niemals | sofort | Die Ausführung des benutzerdefinierten Images wird sofort gestartet. Hierfür ist es erforderlich, dass ein benutzerdefiniertes Image bereits auf der SD-Karte des iRMC S4 verfügbar ist und zur Auswahl angeboten wird. |
| niemals | geplant[1] | Die Ausführung des benutzerdefinierten Images wird geplant gestartet. Hierfür ist es erforderlich, dass ein benutzerdefiniertes Image bereits auf der SD-Karte des iRMC S4 verfügbar ist und zur Auswahl angeboten wird. |

Tabelle 11: Einstellungen für benutzerdefinierte Images

[1] täglich, wöchentlich, monatlich, jährlich, nur einmal

*Abbrechen*

Bricht die Vorbereitung des Downloads ab. *Abbrechen* funktioniert nur, solange der Download nicht gestartet wurde. Nach dem Start des Downloads ist die Schaltfläche *Abbrechen* deaktiviert.

*Ausgewählte Datei Löschen*
: Löscht die ausgewählten Images von der SD-Karte des iRMC S4.

*Unmount Selected Image*
: Hebt die Bereitstellung des ausgewählten Images auf.

### Custom Image Logs

In der Gruppe *Custom Image Logs* wird angezeigt, ob eine Log-Datei in Bezug auf das benutzerdefinierte Image verfügbar ist. Falls dies der Fall ist, können Sie die Log-Datei speichern.

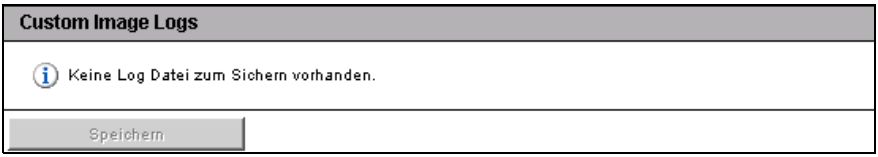



Bild 230: Seite "Online Aktualisierung" – Online Aktualisierungs Logs

*Speichern*
: Öffnet ein Bestätigungsdialogfenster, über das die Log-Datei gespeichert werden kann. Die Schaltfläche *Speichern* ist deaktiviert, wenn keine Log-Datei verfügbar ist.

### 7.18.5 PrimeCollect – Health Management

Auf der Seite *PrimeCollect* können Sie verschiedene PrimeCollect-Archive auf der SD-Karte des iRMC S4 speichern. Außerdem können Sie ein spezielles "Referenz-Image" definieren, das nicht nach dem Ringpufferprinzip überschrieben wird.

Das vom iRMC S4 bereitgestellte Out-of-Band-eLCM erweitert und verbessert die standardmäßige Funktionalität und Verwendbarkeit von PrimeCollect wie folgt:

– PrimeCollect-Archive automatisch und geplant erstellen.

– PrimeCollect-Archivdateien auf der SD-Karte des iRMC S4 speichern. Insbesondere können Sie ein spezielles "Referenz-Image" definieren, das nicht nach dem Ringpufferprinzip überschrieben wird.

– Verlauf der PrimeCollect-Archive verwalten.

– PrimeCollect-Archive über Management LAN oder AIS Connect auf einen anderen Server übertragen.

– Das PrimeCollect-Archiv auf den lokalen Computer herunterladen.

Die Erstellung von PrimeCollect-Archivdateien basiert auf der Kommunikation zwischen dem iRMC S4 und dem ServerView Agentless Service. In der Gruppe *System Informationen* auf der Seite *System Überblick* wird angezeigt, ob der ServerView Agentless Service auf dem Server verfügbar ist (siehe Seite 151).

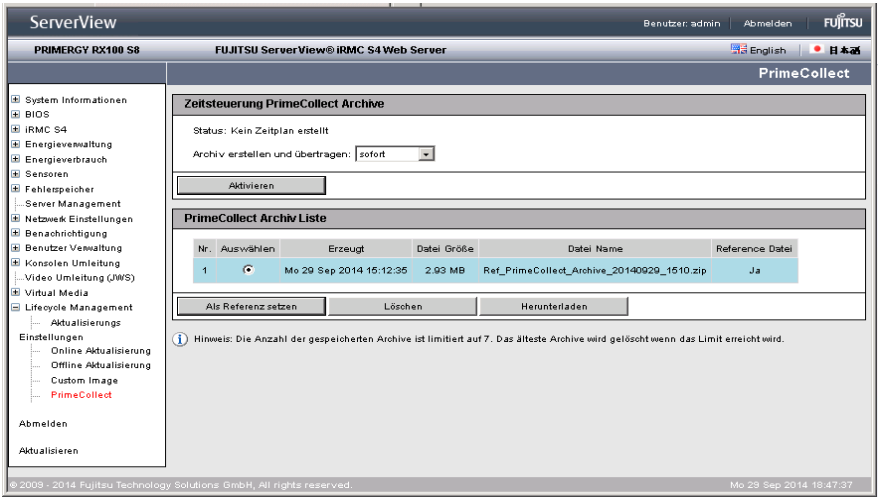



Bild 231: Seite "PrimeCollect" – Zeitsteuerung PrimeCollect Archive

## Zeitsteuerung PrimeCollect Archive

In der Gruppe *Zeitsteuerung PrimeCollect Archive* können Sie die Erstellung und den Download von Archiven konfigurieren.

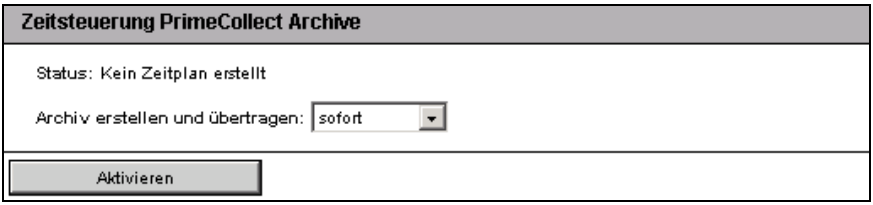



Bild 232: Seite "PrimeCollect"

*Status*

Zeigt den aktuellen Status der Archiverstellung und des Aktualisierungsvorgangs an.

*Archiv erstellen und übertragen*

Hier können Sie konfigurieren, ob durch die Auswahl von *Aktivieren* die Ausführung des benutzerdefinierten Images sofort, automatisch an einem bestimmten Datum oder in regelmäßigen Abständen gestartet wird.

*sofort*
: Führt die Erstellung und den Download von Archiven sofort durch.

*täglich*
: Führt die Erstellung und den Download von Archiven einmal pro Tag zur festgelegten Uhrzeit durch.

*wöchentlich*
: Führt die Erstellung und den Download von Archiven einmal pro Woche am festgelegten Tag zur festgelegten Uhrzeit durch.

*monatlich*
: Führt die Erstellung und den Download von Archiven einmal pro Monat am festgelegten Tag zur festgelegten Uhrzeit durch.

*jährlich*
: Führt die Erstellung und den Download von Archiven einmal pro Jahr am festgelegten Datum durch.

*nur einmal*
: Führt die Erstellung und den Download von Archiven am festgelegten Datum durch.

*niemals*
: Führt niemals eine Erstellung und einen Download von Archiven durch.

*Aktivieren/Deaktivieren*
: Aktiviert/deaktiviert die Konfiguration:

- Wenn Sie auf *Aktivieren* klicken, werden die Erstellung und der Download von Archiven gemäß den Einstellungen gestartet, die unter *Archiv erstellen und übertragen* konfiguriert sind.
- Wenn Sie auf *Deaktivieren* klicken, wird die Erstellung und der Download von Archiven gestoppt, die aktuell verarbeitet werden.

### PrimeCollect Archiv Liste

Unter *PrimeCollect Archiv Liste* wird eine Liste der verfügbaren PrimeCollect-Archive angezeigt.

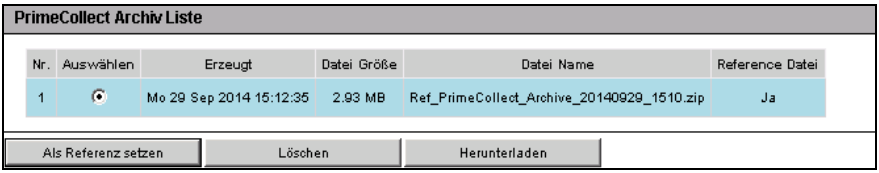



Bild 233: Seite "PrimeCollect" – PrimeCollect Archiv Liste

*Als Referenz setzen*
: Kennzeichnet das aktuell ausgewählte Archiv als das Referenzarchiv. Wenn die Liste nur ein Archiv enthält, wird dieses Archiv automatisch als das Referenzarchiv verwendet.

*Löschen*
: Löscht das ausgewählte Archiv aus der Liste.

*Herunterladen*
: Öffnet den Dialog "File Browser", über den Sie das ausgewählte Archiv öffnen oder speichern können.

# 8 iRMC S4 über Telnet/SSH (Remote Manager)

Für den iRMC S4.ist eine Telnet-basierte Oberfläche vorhanden. Diese ist bekannt als Remote Manager. Den Remote Manager können Sie über jeden Telnet/SSH-Client aufrufen:

Der iRMC S4 unterstützt gesicherte Verbindungen über SSH (**S**ecure **Sh**ell). Die Oberfläche des Remote Manager ist für Telnet und SSH-Verbindungen identisch. Im Prinzip kann jeder Telnet/SSH-Client, der VT100-Sequenzen versteht, für den Zugriff auf den iRMC S4 verwendet werden. Es wird jedoch empfohlen, die iRMC S4-Weboberfläche oder das ServerView Remote Management Frontend (im Folgenden kurz: Remote Management Frontend) zu verwenden.

Im diesem Kapitel sind Bedienung und Funktionen des iRMC S4 über den Remote Manager im Einzelnen beschrieben. Am Ende des Kapitels finden Sie außerdem einen kurzen Überblick über SMASH CLP

## 8.1 Voraussetzung am verwalteten Server

Für den iRMC S4 muss der Zugriff über Telnet aktiviert sein (siehe Abschnitt "Ports und Netzwerk Dienste - Ports und Netzwerk-Dienste konfigurieren" auf Seite 276).

Der Zugang über das Telnet-Protokoll ist aus Sicherheitsgründen standardmäßig deaktiviert, da Passwörter im Klartext übertragen werden.

Da der ServerView Operations Manager den Wert des Management-Ports nicht kennt, arbeitet das Remote Management Frontend mit dem Default-Wert.

Da nach dem Start des Remote Management Frontends nicht automatisch eine Verbindung aufgebaut wird, können Sie einen vom Default-Wert abweichenden Wert für den Management-Port auch noch nach dem Start des Remote Management Frontends korrigieren.

## 8.2 Remote Manager bedienen

Anhand von Bild 234, das einen Ausschnitt aus dem Hauptmenü des Remote Manager zeigt, ist nachfolgend die Bedienung des Remote Manager exemplarisch dargestellt.

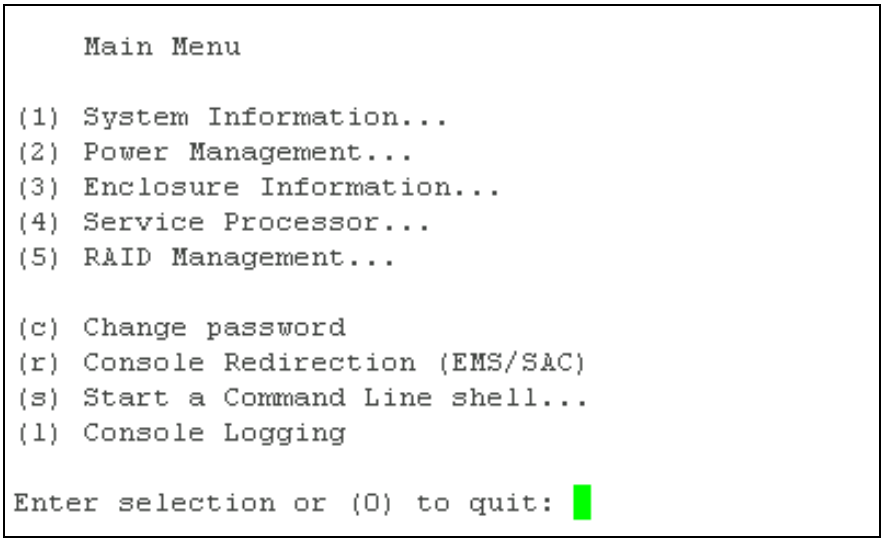



Bild 234: Bedienung des Remote Manager

- Den gewünschten Menüpunkt wählen Sie aus, indem Sie die Ziffer / den Buchstaben eingeben, der diesem Menüpunkt vorangestellt ist (z. B. „c“ für Change password)

  Funktionen, die einem Benutzer nicht erlaubt sind, sind mit einem Gedankenstrich (-) gekennzeichnet, Funktionen, die nicht verfügbar sind, mit einem Stern (*).

- Mit der Taste 0 oder der Tastenkombination Ctrl D beenden Sie den Remote Manager. Es wird ein entsprechendes Ereignis in das Eventlog geschrieben.

## 8.3 Menü-Übersicht

Das Remote Manager Menü für den iRMC S4 ist wie folgt strukturiert:

- **System Information**
  - View Chassis Information
  - View Mainboard Information
  - View OS and SNMP Information
  - Set ASSET Tag
- **Power Management**
  - Immediate Power Off
  - Sofort zurücksetzen
  - Power Cycle
  - Power On
  - Graceful Power Off (Shutdown)
  - Graceful Reset (Reboot)
  - Raise NMI (via iRMC S4)
- **Enclosure Information**
  - System Event-Log
    - View System Eventlog (text, newest first)
    - View System Eventlog (text, oldest first)
    - Dump System Eventlog (raw, newest first)
    - Dump System Eventlog (raw, oldest first)
    - View System Eventlog Information
    - Clear System Eventlog

- Internal Eventlog
  - View Internal Eventlog (text, newest last)
  - Dump Internal Eventlog (raw, newest last)
  - View Internal Eventlog Information
  - Clear Internal Eventlog
  - Change Internal Eventlog mode
- Temperature
- Voltages/Current
- Fans
- Power Supplies
- Memory Sensor
- Door Lock
- CPU Sensors
- Component Status (Lightpath)
- List All Sensors

- **Service Processor**
  - Configure IP Parameters
  - List IP Parameters
  - Toggle Identify LED
  - Reset iRMC S4 (Warm reset)
  - Reset iRMC S4 (Cold reset)
- **RAID Management**
  - Controller information
  - Physical device information
  - Logical device information
  - Array configuration information
  - BBU status

- **Change password**
- **Console Redirection (EMS/SAC)**
- **Start a Command Line shell**
- **Console Logging**

# 8.4 Anmeldeprozess

Wenn Sie sich am iRMC S4 anmelden, müssen Sie Ihre Authentisierungsdaten (Benutzername und Passwort) eingeben. Sobald eine Verbindung zum iRMC S4 aufgebaut ist, wird im Terminal Client am Remote-Arbeitsplatz das Anmeldefenster des Remote Managers (Telnet/SSH-Fenster) angezeigt.

Je nachdem, ob ServerView Agents auf dem System schon einmal gestartet wurden, wird das Anmeldefenster mit oder ohne Systeminformationen angezeigt.

Wenn Sie sich über eine SSH-Verbindung anmelden: Falls der Host-Key des verwalteten Servers noch nicht am Remote-Arbeitsplatz registriert ist, meldet der SSH-Client einen Security-Alert mit Vorschlägen für das weitere Vorgehen.

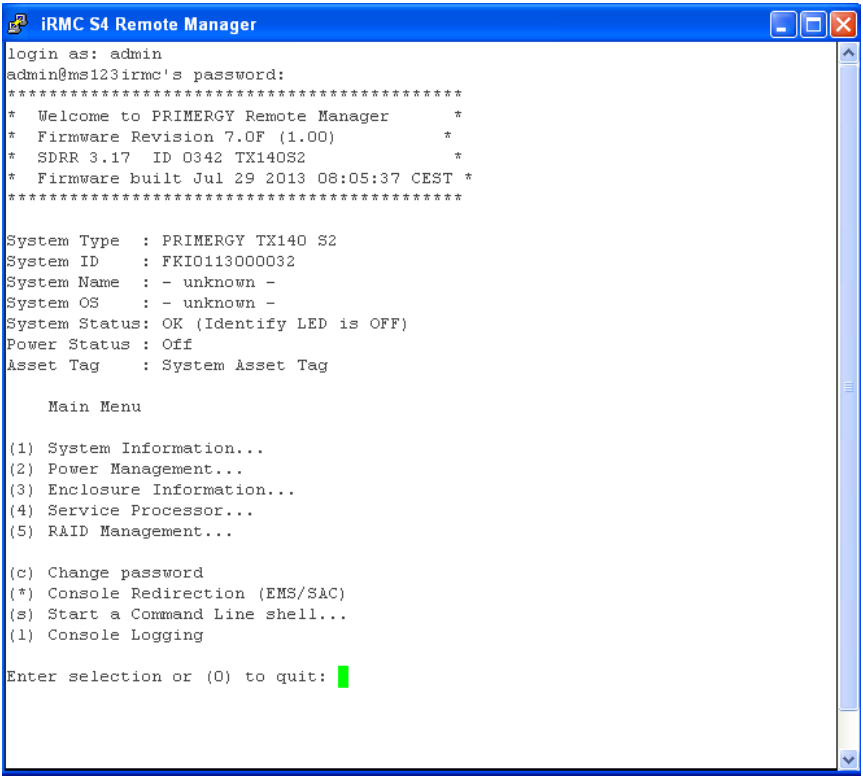

iRMC S4 Remote Manager
login as: admin
admin@ms123irmc's password:
*****************************************
* Welcome to PRIMERGY Remote Manager *
* Firmware Revision 7.0F (1.00) *
* SDRR 3.17 ID 0342 TX140S2 *
* Firmware built Jul 29 2013 08:05:37 CEST *
*****************************************
System Type : PRIMERGY TX140 S2
System ID : FKIO113000032
System Name : - unknown -
System OS : - unknown -
System Status: OK (Identify LED is OFF)
Power Status : Off
Asset Tag : System Asset Tag
Main Menu
(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(5) RAID Management...
(c) Change password
(*) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging
Enter selection or (0) to quit:

Bild 235: Remote Manager: Anmeldefenster (mit Systeminformation)

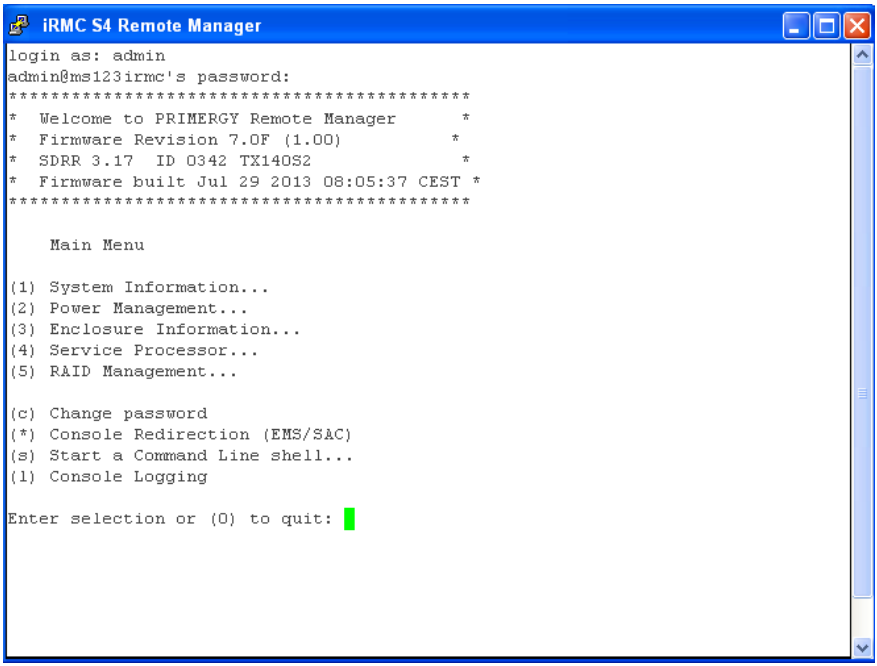

iRMC S4 Remote Manager
login as: admin
admin@ms123irmc's password:
*****************************************
* Welcome to PRIMERGY Remote Manager *
* Firmware Revision 7.0F (1.00) *
* SDRR 3.17 ID 0342 TX140S2 *
* Firmware built Jul 29 2013 08:05:37 CEST *
*****************************************
Main Menu
(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...
(5) RAID Management...
(c) Change password
(*) Console Redirection (EMS/SAC)
(s) Start a Command Line shell...
(l) Console Logging
Enter selection or (0) to quit:

Bild 236: Remote Manager: Anmeldefenster (ohne Systeminformation)

Das Fenster „Remote Manager“ enthält Informationen zum betroffenen System. Anhand dieser Informationen können Sie den Server und den Betriebsstatus identifizieren. Einige Angaben (z. B. der System Name) werden nur für Server angezeigt und nur dann, wenn der Server entsprechend konfiguriert ist.

- Um den Remote Manager zu nutzen, müssen Sie sich mit einer Benutzerkennung und einem Passwort anmelden.

  Anschließend wird ein entsprechendes Ereignis in das Eventlog geschrieben und das entsprechende Hauptmenü des Remote Manager angezeigt (siehe Abschnitt "Hauptmenü des Remote Manager" auf Seite 394).

  Sie können den Anmeldevorgang vorzeitig mit Ctrl D beenden.

# 8.5 Hauptmenü des Remote Manager

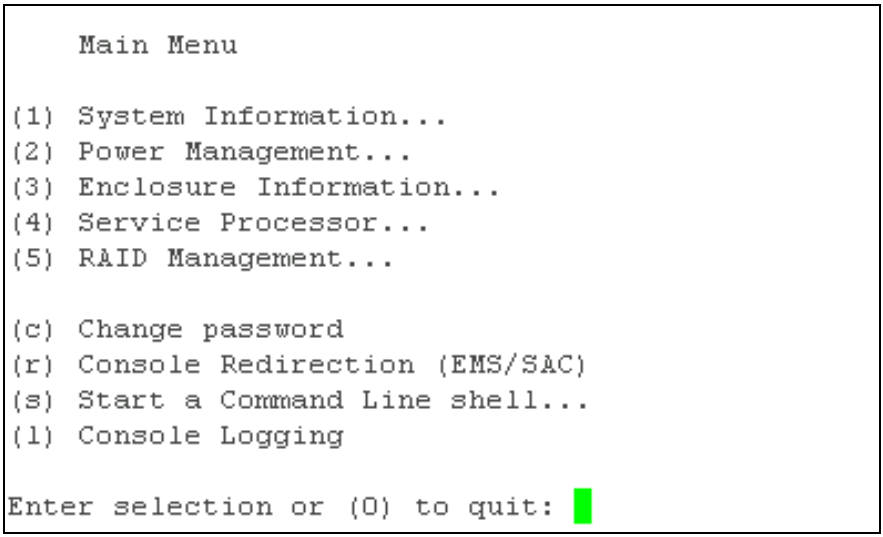



Bild 237: Remote Manager: Hauptmenü

Das Hauptmenü des Remote Manager bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *System Information...* | Informationen zum verwalteten Server einsehen und den Asset Tag (Bestandskennzeichen) setzen (siehe Abschnitt "System Informationen - Informationen zum verwalteten Server" auf Seite 398) |
| *Power Management...* | Server ein/ausschalten (siehe Abschnitt "Power Management" auf Seite 399) |

Tabelle 12: Hauptmenü des Remote Manager

| | |
|---|---|
| *Enclosure Information...* | Informationen über den aktuellen Systemzustand anfordern, z. B. Fehler- und Ereignismeldungen von Error-Log und Eventlog überprüfen (Temperatur, Lüfter, ...)<br>(siehe Abschnitt "Enclosure Information - Systemeventlog und Status der Sensoren" auf Seite 400) |
| *Service Processor...* | Den iRMC S4 konfigurieren (z. B. Firmware aktualisieren oder IP-Adresse ändern)<br>(siehe Abschnitt "Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S4" auf Seite 404) |
| *RAID Management...* | Informationen zu RAID Controller, physikalischen und logischen Geräten, Array-Konfiguration und BBU-Status.<br>(siehe Abschnitt "RAID Management" auf Seite 405) |
| *Change password* | Passwortwort ändern<br>(siehe Abschnitt "Passwortwort ändern" auf Seite 398) |
| *Console Redirection (EMS/SAC)* | Text-Konsolen-Umleitung<br>(siehe Abschnitt "Console Redirection (EMS/SAC) - Text-Konsolen-Umleitung starten" auf Seite 406) |
| *Start a Command Line shell...* | Command Line Shell starten<br>(siehe Abschnitt "Start a Command Line shell... - SMASH CLP Shell starten" auf Seite 406) |
| *Console Logging* | Meldungsausgabe auf die Text-Konsole steuern<br>(siehe Abschnitt "Console Logging - Meldungsausgabe auf die Text-Konsole (seriell)" auf Seite 407) |

Tabelle 12: Hauptmenü des Remote Manager

# 8.6 Erforderliche Benutzerberechtigungen

Tabelle 13 gibt einen Überblick, welche Benutzerberechtigungen zur Nutzung der einzelnen Funktionen des Remote Manager erforderlich sind.

| Menüpunkte des Remote Manager | Zulässig mit IPMI Privilege Level | | | | Erforderliche Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC S4-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| Ansehen *System Information...* | X | X | X | X | | | | |
| View Chassis / Mainboard / OS Information | | | | | | X | | |
| Set ASSET Tag[1)] | | | | | | X | | |
| Set System Name [1)] | | | | | | X | | |
| Set System Operating System Information[1)] | | | | | | X | | |
| Set System Description[1)] | | | | | | X | | |
| Set System Location Information (SNMP)[1)] | | | | | | X | | |
| Set System Contact Information (SNMP)[1)] | | | | | | X | | |
| *Power Management...* | X | X | X | | | | | |
| Ansehen *Enclosure Information* | X | X | X | X | | | | |
| *System Eventlog - View/Dump System Eventlog* | X | X | X | X | | | | |
| *System Eventlog - Clear System Eventlog* | X | X | X | | | | | |
| *Internal Eventlog - View/Dump Internal Eventlog* | X | X | X | X | | | | |
| *Internal Eventlog - Clear Internal Eventlog* | X | X | X | X | | | | |
| *Sensor-Übersichten (Temperature, Fans ...)* | X | X | X | X | | | | |
| Ansehen *Service Processor...* | X | X | X | X | | | | |

Tabelle 13: Berechtigungen zur Nutzung des Remote Manager-Menüs

| Menüpunkte des Remote Manager | Zulässig mit IPMI Privilege Level | | | | Erforderliche Berechtigung | | | |
|---|---|---|---|---|---|---|---|---|
| | OEM | Administrator | Operator | User | Benutzerkonfiguration erlaubt | iRMC S4-Einstellungen konfigurieren | Konsolenumleitung erlaubt | Remote Storage erlaubt |
| *Service Processor... - List IP Parameters* | | | | | | X | | |
| *Service Processor... - Configure IP Parameters* | | | | | | X | | |
| *Service Processor... - Toggle Identify LED* | X | X | X | X | | | | |
| *Service Proc. ... - Reset iRMC S4 (warm/cold reset)* | X | X | | | | | | |
| Anzeige *RAID Management*.2) | X | X | | | | | | |
| View Controller information2) | X | X | | | | | | |
| View physical device information2) | X | X | | | | | | |
| View logical device information2) | X | X | | | | | | |
| View array configuration information2) | X | X | | | | | | |
| View BBU status 2 | X | X | | | | | | |
| *Change password* | | | | | X | | | |
| Console Redirection (EMS/SAC) | X | X | X | | | | | |
| Start a Command Line shell... | X | X | X | X | | | | |
| Console Logging | X | X | X | | | | | |

[1)] Die Aktion ist nur möglich, wenn keine Agenten gestartet sind
2) Systemabhängige Funktion

Tabelle 13: Berechtigungen zur Nutzung des Remote Manager-Menüs

## 8.7 Passwortwort ändern

Mit dem Menüpunkt *Change password* kann ein Benutzer mit der Berechtigung *Benutzerkonfiguration erlaubt* (siehe Seite 65) tsein eigenes Passwort sowie die Passwörter anderer Benutzer ändern.

## 8.8 System Informationen - Informationen zum verwalteten Server

Wenn Sie im Hauptmenü den Menüpunkt *System Information..* auswählen, erhalten Sie das folgende Menü:

```
    System Information Menu

(1) View Chassis Information
(2) View Mainboard Information
(3) View OS and SNMP Information

(4) Set ASSET Tag
(*) Set System Name
(*) Set System Operating System Information
(*) Set System Description
(*) Set System Location Information (SNMP)
(*) Set System Contact Information (SNMP)

Enter selection or (0) to quit:
```

Bild 238: Remote Manager: Menü System Information

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *View Chassis Information* | Informationen über das Gehäuse des verwalteten Servers und seine Produktdaten. |
| *View Mainboard Information* | Informationen zur Systembaugruppe des verwalteten Servers und ihren Produktdaten. |
| *View OS and SNMP Information* | Informationen zum Betriebssystem und zur ServerView-Version des verwalteten Servers und zu den SNMP-Einstellungen |
| *Set ASSET Tag* | Kundenspezifischen Asset-Tag für den verwalteten Server setzen. |

Tabelle 14: Menü System Information

# 8.9 Power Management

Wenn Sie im Hauptmenü den Menüpunkt *Power Management...* auswählen, erhalten Sie das folgende Menü:

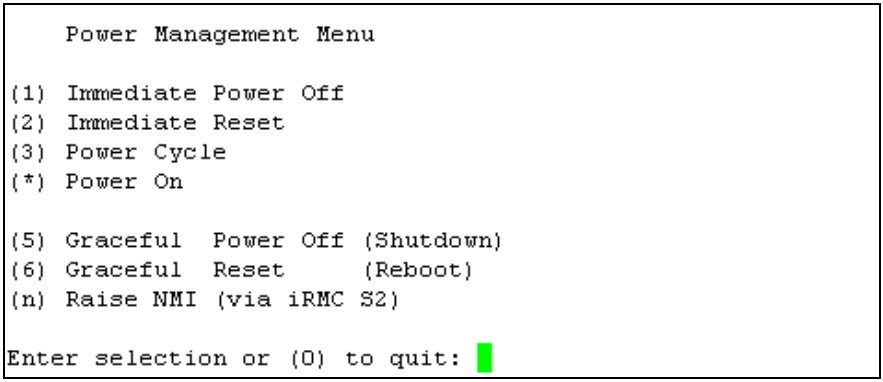

Power Management Menu
(1) Immediate Power Off
(2) Immediate Reset
(3) Power Cycle
(*) Power On
(5) Graceful Power Off (Shutdown)
(6) Graceful Reset (Reboot)
(n) Raise NMI (via iRMC S2)
Enter selection or (0) to quit:

Bild 239: Remote Manager: Menü Power Management

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *Immediate Power Off* | Schaltet den Server aus unabhängig vom Status des Betriebssystems aus. |
| *Sofort zurücksetzen* | Startet den Server unabhängig vom Status des Betriebssystems komplett neu (Kaltstart). |
| *Power Cycle* | Schaltet den Server vollständig aus und nach einer konfigurierten Zeit automatisch wieder ein. |
| *Power On* | Schaltet den Server ein. |
| *Graceful Power Off (Shutdown)* | System „sanft“ herunterfahren und ausschalten. Der Menüpunkt ist nur verfügbar, wenn ServerView Agents installiert und beim iRMC S4 als „connected“ gemeldet sind. |
| *Graceful Reset (Reboot)* | Graceful Shutdown und Reboot. Der Menüpunkt ist nur verfügbar, wenn ServerView Agents installiert und beim iRMC S4 als „connected“ gemeldet sind. |

Tabelle 15: Menü Power Management

# 8.10 Enclosure Information - Systemeventlog und Status der Sensoren

Wenn Sie im Hauptmenü den Menüpunkt *Enclosure Information...* auswählen, erhalten Sie das folgende Menü:

```
    Enclosure Information Menu

(e) System Eventlog
(i) Internal Eventlog
(t) Temperature
(v) Voltages/Current
(f) Fans
(p) Power Supplies
(d) Door Lock
(m) Memory Sensors
(c) CPU Sensors
(s) Component Status
(l) List All Sensors

Enter selection or (0) to quit:
```

Bild 240: Remote Manager: Menü Enclosure Information

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *System Event-Log* | Ruft das Menü *System Eventlog* auf (siehe Abschnitt "System Event-Log" auf Seite 402). |
| *Internal Eventlog* | Ruft das Menü *Internal Eventlog* auf (siehe Abschnitt"Internal Eventlog" auf Seite 403). |
| *Temperature* | Informationen über die Temperatur-Sensoren und deren Status anzeigen. |
| *Voltages/Current* | Informationen über die Spannungs- und Strom-Sensoren und deren Status anzeigen. |
| *Fans* | Informationen über die Lüfter und deren Status anzeigen. |
| *Power Supplies* | Informationen über die Netzteile und deren Redundanz-Status anzeigen. |
| *Door Lock* | Informationen anzeigen, ob Front oder Gehäuse geöffnet sind. |
| *Memory Sensors* | Informationen zu den Status der Speichersensoren anzeigen. |
| *CPU Sensors* | Prozessor(en) des Servers lokalisieren. |
| *Component Status* | Detail-Informationen zu allen Sensoren anzeigen, die über eine PRIMERGY Diagnostic LED verfügen. |
| *List All Sensors* | Detail-Informationen zu allen Sensoren anzeigen. |

Tabelle 16: Menü Enclosure Information

### System Event-Log

Wenn Sie im Untermenü *Enclosure Information...* den Menüpunkt *System Eventlog* auswählen, erhalten Sie das folgende Menü:

```
    System Eventlog Menu

(1) View System Eventlog (text, newest first)
(2) View System Eventlog (text, oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)

(5) View System Eventlog Information
(6) Clear System Eventlog

Enter selection or (0) to quit:
```

Bild 241: Remote Manager: Menü System Eventlog

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *View System Eventlog (text, newest first)* | Der Inhalt des Fehlerspeichers (System Eventlog) wird in lesbarer Form und chronologischer Reihenfolge am Bildschirm ausgegeben (der jüngste Eintrag zuerst). |
| *View System Eventlog (text, oldest first)* | Der Inhalt des Fehlerspeichers wird in lesbarer Form und umgekehrter chronologischer Reihenfolge am Bildschirm ausgegeben (der älteste Eintrag zuerst). |
| *Dump System Eventlog (raw, newest first)* | Der Inhalt des Fehlerspeichers wird in chronologischer Reihenfolge ausgeschrieben (der jüngste Eintrag zuerst). |
| *Dump System Eventlog (raw, oldest first)* | Der Inhalt des Fehlerspeichers wird in umgekehrt chronologischer Reihenfolge ausgeschrieben (der älteste Eintrag zuerst). |
| *View System Eventlog Information* | Informationen zum Fehlerspeicher. |
| *Clear System Eventlog* | Der Inhalt des Fehlerspeichers wird gelöscht. |
| *Change System Eventlog mode* | Ändert den Puffer-Modus des Fehlerspeichers vom Modus *Ring Buffer* in den Modus *Linear Buffer* und umgekehrt. |

Tabelle 17: Menü System Eventlog

### Internal Eventlog

Wenn Sie im Untermenü *Enclosure Information..* den Menüpunkt *Internal Eventlog* auswählen, erhalten Sie das folgende Menü:

```
    Internal Eventlog Menu

(1) View Internal Eventlog (text, newest last)
(2) Dump Internal Eventlog (raw, newest last)
(3) View Internal Eventlog Information
(4) Clear Internal Eventlog
(5) Change Internal Eventlog mode

Enter selection or (0) to quit:
```

Bild 242: Remote Manager: Menü Internal Eventlog

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *View Internal Eventlog (text, newest last)* | Der Inhalt des internen Ereignisspeichers (internal Eventlog) wird in lesbarer Form und umgekehrter chronologischer Reihenfolge am Bildschirm ausgegeben (der neueste Eintrag zuletzt). |
| *Dump Internal Eventlog (raw, newest last )* | Der Inhalt des internen Ereignisspeichers wird in umgekehrt chronologischer Reihenfolge am Bildschirm ausgegeben (der neueste Eintrag zuletzt). |
| *View Internal Eventlog Information* | Informationen zum internen Ereignisspeicher. |
| *Clear Internal Eventlog* | Inhalt des internen Ereignisspeichers wird gelöscht. |
| *Change Internal Eventlog mode* | Ändert den Puffer-Modus des internen Ereignisspeichers vom Modus *Ring Buffer* in den Modus *Linear Buffer* und umgekehrt. |

Tabelle 18: Menü Internal Eventlog

# 8.11 Service Processor - IP-Parameter, Identifizierungs-LED und Reset des iRMC S4

Wenn Sie im Hauptmenü den Menüpunkt *Enclosure Information...* auswählen, erhalten Sie das folgende Menü:

```
    Service Processor Menu

(1) Configure IP Parameters
(2) List IP Parameters

(3) Toggle Identify LED

(4) Reset iRMC S2 (Warm reset)
(5) Reset iRMC S2 (Cold reset)

Enter selection or (0) to quit:
```

Bild 243: Remote Manager: Menü Service Processor

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *Configure IP Parameters* | IPv4 / IPv6-Adressen des iRMC S4 konfigurieren. Zu Details für die Einzelnen Einstellungen siehe Abschnitt "Netzwerk Schnittstelle - Ethernet-Einstellungen des iRMC S4 konfigurieren" auf Seite 269. |
| *List IP Parameters* | IP-Einstellungen anzeigen. |
| *Toggle Identify LED* | PRIMERGY Identifizierungs-LED ein-/ausschalten. |
| *Reset iRMC S4 (Warm reset)* | iRMC S4 zurücksetzen. Die Verbindung wird beendet.<br>Es werden nur die Schnittstellen neu initialisiert. |
| *Reset iRMC S4 (Cold reset)* | iRMC S4 zurücksetzen. Die Verbindung wird beendet.<br>Der iRMC S4 wird komplett neu initialisiert. |

Tabelle 19: Menü Service Processor

Es wird empfohlen, nach einem *Reset iRMC S4 (Cold Reset)* oder *Reset iRMC S4 (Warm Reset)* den Server neu zu starten (siehe Seite 404).

## 8.12 RAID Management

Wenn Sie im Hauptmenü *RAID Management...* wählen, wird das folgende Menü angezeigt:

```
    RAID Management Menu

(1) Controller information
(2) Physical device information
(3) Logical device information
(4) Array configuration information
(5) BBU status

Enter selection or (0) to quit:
```

Bild 244: Remote Manager: Menü Service Processor

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *Controller Information* | Enthält Informationen zu jedem RAID Controller auf dem verwalteten Server. |
| *Physical Device Information* | Enthält Informationen zu jedem RAID Physikalischen Laufwerk auf dem verwalteten Server. |
| *Logical Device Information* | Enthält Informationen zu jedem RAID Logischen Laufwerk auf dem verwalteten Server. |
| *Array configuration information* | Enthält Informationen zur Array-Konfiguration. |
| *BBU status* | Enthält Informationen zum Status der Battery Backup Units (BBU). |

Tabelle 20: Menü Service Processor

## 8.13 Console Redirection (EMS/SAC) - Text-Konsolen-Umleitung starten

Unter dem Menüpunkt *Console Redirection (EMS/SAC)* des Hauptmenüs können Sie die Text-Konsolen-Umleitung starten.

Die Text basierte Console Redirection funktioniert via LAN nur mit Serial 1.

Falls die Console Redirection auch bei laufendem Betriebssystem genutzt werden soll, muss der *Serial 1 Multiplexer* auf *System* konfiguriert sein.

Verwenden Sie die Tastaturbefehle „<ESC>(“ oder „~.“ (Tilde Punkt), um die Textkonsole zu schließen.

Je nach Typ des PRIMERGY Servers funktioniert unter Umständen nur eine dieser beiden Möglichkeiten.

## 8.14 Start a Command Line shell... - SMASH CLP Shell starten

*Start a Command Line shell...* im Hauptmenü startet eine SMASH CLP Shell. SMASH CLP ist die Abkürzung für “**S**ystems **M**anagement **A**rchitecture for **S**erver **H**ardware **C**ommand **L**ine **P**rotocol”. Dieses Protokoll ermöglicht eine Verbindung zwischen der Management-Station und dem verwalteten Server auf Basis von Telnet oder SSH. Näheres zu SMASH CLP finden Sie im Abschnitt "Command Line Protocol (CLP)" auf Seite 409.

Wenn Sie im Hauptmenü den Menüpunkt *(s) Start a Command Line shell...* auswählen, wird das folgende Fenster angezeigt:

```
    Shell Menu

(1) Start SMASH CLP shell...


Enter selection or (0) to quit:
```

Bild 245: Remote Manager: Menü „SMASH CLP Shell starten...“

- Wählen Sie *(1) Start a SMASH CLP shell...*, um die SMASH CLP Shell zu starten.

# 8.15 Console Logging - Meldungsausgabe auf die Text-Konsole (seriell)

Unter dem Menüpunkt *Console Logging* des Hauptmenüs können Sie die Meldungsausgabe (Logging) auf die Text-Konsole (serielle Schnittstelle) steuern.

Wenn Sie im Hauptmenü den Menüpunkt *(l) Console Logging* auswählen, wird das folgende Fenster angezeigt:

```
    Console Logging Menu

(1) Change Logging Run state
(2) Clear Console Logging buffer
(3) Replay Console (Fast mode)
(4) Replay Console (Continuous mode)

Enter selection or (0) to quit:
```

Bild 246: Remote Manager: Menü Console Logging

Das Untermenü bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *Change Logging Run state* | Ausführungsstatus des Console Logging anzeigen und steuern.<br>Näheres siehe "Console Logging Run State Menu" auf Seite 408 |
| *Clear Console Logging buffer* | Console Logging-Puffer löschen. |
| *Replay Console (Fast mode)* | Console Logging anzeigen (Schnellmodus) |
| *Replay Console (Continuous mode)* | Console Logging anzeigen (kontinuierlicher Modus) |

Tabelle 21: Menü Console Logging

### Console Logging Run State Menu

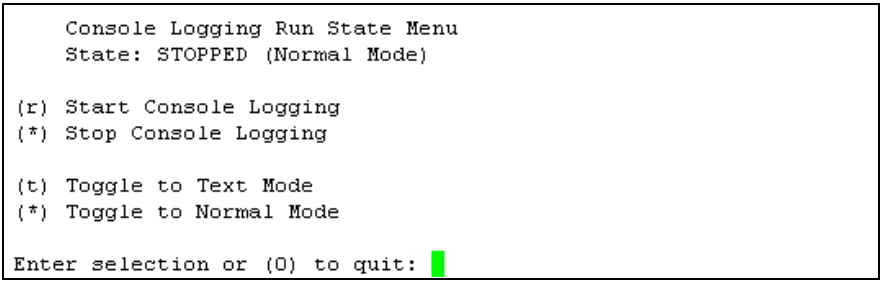

Console Logging Run State Menu
State: STOPPED (Normal Mode)
(r) Start Console Logging
(*) Stop Console Logging
(t) Toggle to Text Mode
(*) Toggle to Normal Mode
Enter selection or (0) to quit:

Bild 247: Remote Manager: Menü Console Logging Run State

Das *Console Logging Run State Menu* bietet Ihnen folgende Funktionen:

| | |
|---|---|
| *Start Console Logging* | Logging auf die Text-Konsole starten. |
| *Stop Console Logging* | Logging auf die Text-Konsole stoppen. |
| *Toggle to Text Mode* | In den Text-Modus schalten.<br>Im Text-Modus werden vor der Ausgabe auf Konsole alle Escape-Sequenzen herausgefiltert. |
| *Toggle to Normal Mode* | In den Normal-Modus schalten.<br>In normal mode, only the following escape sequences are filtered out before messages are output to the console:<br><ESC>(<br><ESC>stop<br><ESC>Q<br><ESC>R<ESC>r<ESC>R<br><ESC>^<br>Damit ist in eingeschränktem Umfang auch Farbe, Pseudo-Grafik etc. darstellbar. |

Tabelle 22: Menü Console Logging Run State

# 8.16 Command Line Protocol (CLP)

Der iRMC S4 unterstützt verschiedene Text-basierte Benutzerschnittstellen, so genannte Benutzer-Shells, die für die einzelnen Benutzer unterschiedlich konfiguriert werden können.

Die Initiative **S**ystem **M**anagement **A**rchitecture for **S**erver **H**ardware (SMASH) definiert eine Reihe von Spezifikationen mit folgenden Zielen:

– Bereitstellung standardisierter Schnittstellen für das Management heterogener Rechnerlandschaften.

– Bereitstellung eines Architektur-Framework mit einheitlichen Schnittstellen, Hardware- und Software-Erkennung, Resource Addressing und Datenmodellen.

Weitere Informationen über SMASH finden unter folgendem Link:

*http://www.dmtf.org/standards/smash*

### SMASH CLP-Syntax

SMASH CLP spezifiziert eine allgemeine Kommandozeilen-Syntax und Meldungsprotokoll-Semantik für das Management von Rechnern im Internet sowie im Umfeld von Unternehmen und Service Providern. Detaillierte Informationen zum SMASH CLP finden Sie in dem DMTF Dokument „Server Management Command Line Protocol Specification (SM CLP)DSP0214“.

Die allgemeine Syntax des CLP lautet wie folgt:

```
<verb> [<options>] [<target>] [<properties>]
```

<verb>

Verben spezifizieren, welches Kommando oder welche Aktion auszuführen ist. The list of verbs describes the following activities, for instance:

– Daten generieren (*set*) und wiedergewinnen (*show*),

– Status eines Ziels ändern (*reset*, *start*, *stop*),

– aktuelle Sitzung steuern (*cd*, *version*, *exit*),

– Informationen zu Kommandos liefern (*help*).

In iRMC S4-Systemen ermöglicht das Kommando *oemfujitsu* auch den Einsatz spezieller OEM-Kommandos.

<options>

Command options modify the action or the behavior of a verb. Options dürfen in einer Kommandozeile unmittelbar hinter dem Verb stehen und müssen immer mit einem vorangehenden Bindestrich („-“) angegeben werden.

Mithilfe von Options können Sie z. B.

- das Ausgabeformat festlegen,
- die rekursive Ausführung des Kommandos zulassen,
- die Version des Kommandos anzeigen lassen oder
- Hilfe-Informationen anfordern.

<target>

<target> spezifiziert die Adresse oder den Pfad des von dem Kommando zu manipulierenden Objekts, d. h. des Kommandoziels. Dies kann ein einzelnes überwachtes Element (Managed Element) sein, wie z. B. eine Festplatte, eine Netzkarte (Network Interface Card, NIC), oder das Administrationsprogramm (Management Assistance Program, MAP) selbst. Als mögliches Ziel kommen aber u. a. auch Services infrage, wie beispielsweise ein Transport-Service.

Unter einem <target> lassen sich mehrere Managed Elements zusammenfassen, deren Verwaltung vom Administrationsprogramm unterstützt wird, z. B. das System als Ganzes.

Pro Kommando darf nur ein einziges <target> angegeben werden.

<properties>

<properties> beschreiben die Eigenschaften des Kommandoziels, die zur Ausführung des Kommandos erforderlich sind. So identifizieren die <properties> über die Klasse des Kommandoziels die Properties im Zielobjekt, deren Werte vom Kommando ermittelt oder modifiziert werden.

### Benutzerdaten im CLP (Überblick)

Die Daten innerhalb des CLP sind hierarchisch angeordnet. Mithilfe des Kommandos *cd* können Sie innerhalb dieser Struktur navigieren.

Bild 248 gibt einen Überblick über die Benutzerdaten im CLP.. Die Namen in den Rechtecken bezeichnen Kommandoziele. Auf jeder Ebene der Hierarchie zeigt das Kommando bzw. Verb *show* die verfügbaren Ziele (Targets), Properties und Verben an.

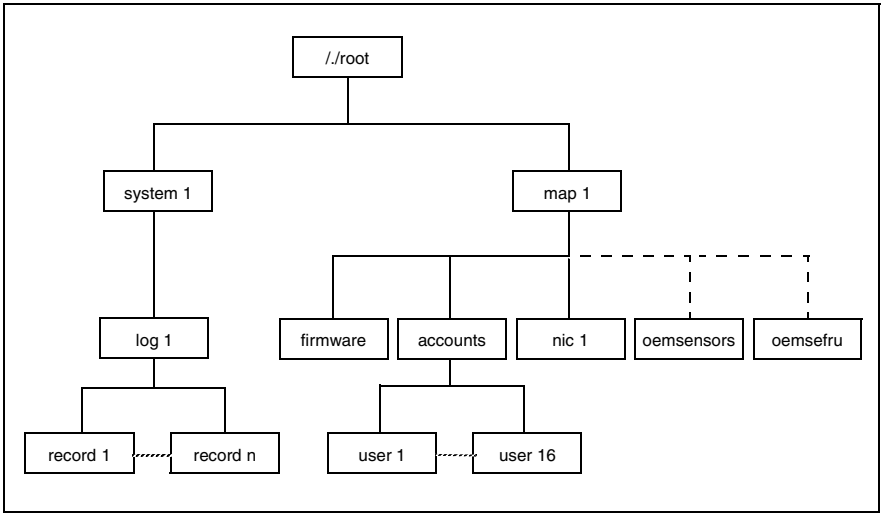



Bild 248: Struktur der Benutzerdaten in SMASH CLP

### Hierarchie der CLP-Kommandos

Tabelle 23 auf Seite 412 gibt einen Überblick über die Hierarchie der CLP-Kommandos..

| Verb / Target | Properties | Comment | cd | show | help | exit | version | set | reset | start | stop | load | oemfsc |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| /<br>**system1**<br>**map1** | | Root | X | X | X | X | X | | | | | | |
| **system1** | name<br>enabledstate | Host System | X | X | X | X | X | | System | PON | POFF | | |
| **...log1** | | Event Log (SEL) | X | X | X | X | X | | iRMC | | | | X |
| **....record<n>** | number<br>date<br>time<br>sensordescription<br>eventdescription<br>eventdirection | Single SEL entry | X | X | X | X | X | | iRMC | | | | X |
| **map1** | name | iRMC | X | X | X | X | X | | iRMC | | | | X |
| **...firmware** | version | iRMC FW | X | X | X | X | X | | iRMC | | | X | X |
| **...accounts** | | Accounts | X | X | X | X | X | X | iRMC | | | | X |
| **.....user<n>** | username<br>password<br>group | User | X | X | X | X | X | X | iRMC | | | | X |
| **...nic1** | networkaddress<br>oemfso_nonvol_networkaddress<br>oemfso_mask<br>oemfso_nonvol_mask<br>oemfso_gateway<br>oemfso_nonvol_gateway<br>oemfso_dhcp_enable<br>oemfso_nonvol_dhcp_enable<br>oemfso_vsi_path<br>oemfso_vsi_server<br>oemfso_vsi_permission<br>oemfso_vsi_sustain | LAN | X | X | X | X | X | X | iRMC | | | | X |
| **...oemfso_sensors** | | OEM Sensors | X | X | X | X | X | | iRMC | | | | X |
| **.....oemfso_sensor_num<n>lun<m>** | oemfso _reading<br>oemfso _status<br>oemfso _sensortype<br>oemfso _readingtype | Single Sensor | X | X | X | X | X | | iRMC | | | | X |
| **...oemfso_frus** | | FRU | X | X | X | X | X | | iRMC | | | | X |
| **.....oemfso_fru_devid<n>lun<m>** | oemfso _description | Single FRU | X | X | X | X | X | | iRMC | | | | X |

Tabelle 23: Hierarchie der CLP-Kommandos

# 9 iRMC S4 via Server Configuration Manager konfigurieren

Mit dem Server Configuration Manager können Sie folgende Aufgaben durchführen:

- Energieverbrauchssteuerung via iRMC S4 auf dem verwalteten Server konfigurieren
- Redundanz der Stromversorgung via iRMC S4 auf dem verwalteten Server konfigurieren
- AVR-Titel, Lizenzschlüssel und andere Funktionen am iRMC S4 konfigurieren
- iRMC S4-Zeiteinstellungen konfigurieren
- den iRMC für die Bereitstellung von Virtual Media konfigurieren
- iRMC S4-DNS-Registrierung konfigurieren
- iRMC S4-DNS-Server konfigurieren
- iRMC S4-E-Mail-Benachrichtigung konfigurieren
- iRMC S4-E-Mail-Formateinstellungen konfigurieren
- iRMC S4-SNMP-Benachrichtigung konfigurieren
- lokale Benutzerverwaltung am iRMC S4 konfigurieren
- einen Directory Server für den iRMC S4 konfigurieren
- den CAS Service am iRMC S4 konfigurieren

**Voraussetzung**:

Auf dem verwalteten Server sind die aktuellen ServerView Agents installiert.

Für den Zugang zur Server Configuration Manager-Funktionalität bieten sich folgende Möglichkeiten:

- Lokal am verwalteten Server über den ServerView Installation Manager (im Folgenden kurz: Installation Manager).
- Lokal am verwalteten Windows-basierten Server über das Windows Startmenü.

Dies wird nur für Server unterstützt, auf denen die ServerView Agents für Windows installiert sind.

– Am Remote-Arbeitsplatz über die grafische Oberfläche des Operations Managers.

Dies wird nur für Server unterstützt, auf denen die ServerView Agents für Windows installiert sind.

Dieses Kapitel beschreibt die verschiedenen Möglichkeiten, den Server Configuration Manager aufzurufen.

Näheres zu den einzelnen Dialogen des Server Configuration Managers finden Sie in der Online-Hilfe des Server Configuration Managers.

## 9.1 Server Configuration Manager via ServerView Installation Manager aufrufen

Den Server Configuration Manager können Sie über den ServerView Installation Manager (im Folgenden kurz Installation Manager) aufrufen. Die Konfiguration via Installation Manager ist bei der Installation des Servers von Bedeutung. Der Installation Manager stellt den Server Configuration Manager sowohl im Rahmen der Installationsvorbereitung als auch als eigenes Wartungsprogramm zur Verfügung. Der Installation Manager ist beschrieben im Handbuch „ServerView Installation Manager“.

## 9.2 Server Configuration Manager über das Windows Startmenü aufrufen

Bei Windows-basierten Servern können Sie den Server Configuration Manager auch über das Windows Startmenü aufrufen.

Gehen Sie hierbei wie folgt vor:

- Wählen Sie am verwalteten Server:
  *Start – All Programs – Fujitsu – ServerView – Agents – Configuration Tools – System Configuration.*

  Das Fenster *System Configuration* öffnet sich:

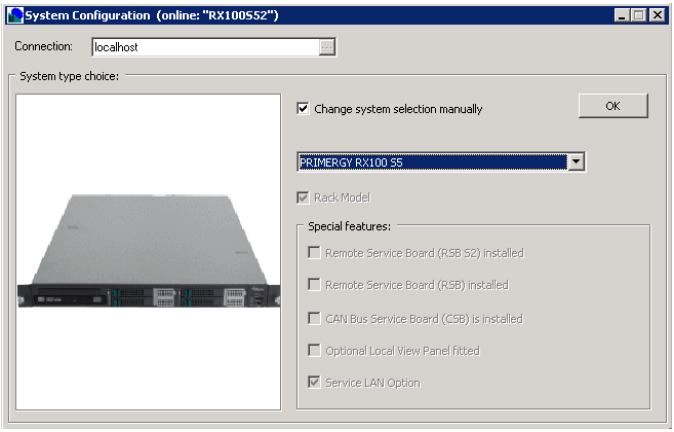



Bild 249: Fenster System Configuration

- ► Übernehmen Sie die voreingestellten Werte.
- ► Klicken Sie auf *OK*.

  Die 'Registerkarten-Ansicht' des Fensters *System Configuration* wird geöffnet.

  Durch Klicken auf die Pfeile links neben der Leiste der Registerkarten können Sie in der Leiste nach links bzw. rechts blättern.

### Einstellungen übernehmen

Um die in den einzelnen Registerkarten vorgenommenen Einstellungen zu übernehmen, verfahren Sie pro Registerkarte wie folgt:

- ► Klicken Sie auf die Schaltfläche *Apply*.
- ► Klicken Sie auf die Schaltfläche *Save Page*.

  Damit die Änderungen der Einstellungen wirksam werden, bootet der iRMC S4 automatisch neu.

## 9.3 Server Configuration Manager über den Operations Manager aufrufen

Die Dialoge des Server Configuration Managers zur Konfiguration des iRMC S4 stehen Ihnen auch über die grafische Oberfläche des Operations Managers zur Verfügung. Damit können Sie den iRMC S4 des verwalteten Servers vom Remote-Arbeitsplatz aus via Web-Interface konfigurieren.

Gehen Sie wie folgt vor:

- ► Starten Sie den Operations Manager (siehe Handbuch „ServerView Operations Manager“).

  Das Startfenster des Operation Managers wird geöffnet:

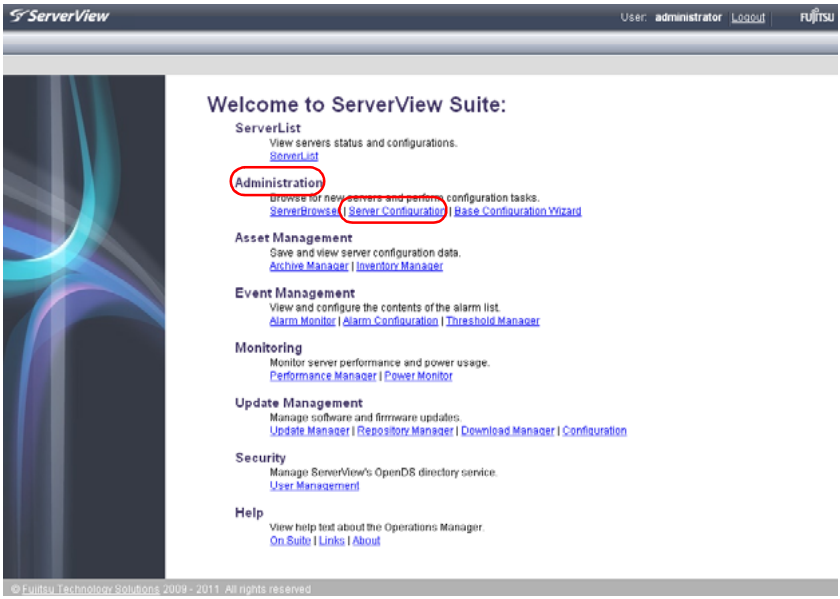

ServerView
User: administrator Logout
FUJITSU
Welcome to ServerView Suite:
ServerList
View servers status and configurations.
ServerList
Administration
ServerBrowser | Server Configuration | Base Configuration Wizard
Asset Management
Save and view server configuration data.
Archive Manager | Inventory Manager
Event Management
View and configure the contents of the alarm list.
Alarm Monitor | Alarm Configuration | Threshold Manager
Monitoring
Monitor server performance and power usage.
Performance Manager | Power Monitor
Update Management
Manage software and firmware updates.
Update Manager | Repository Manager | Download Manager | Configuration
Security
Manage ServerView's OpenDS directory service.
User Management
Help
View help text about the Operations Manager.
On Suite | Links | About
© Fujitsu Technology Solutions 2009 - 2011 All rights reserved

Bild 250: Operations Manager: Startfenster

► Wählen Sie im Menü des Operations Manager-Startfensters unter *Administration* den Menüpunkt *Server Configuration*.

Das folgende Fenster wird angezeigt:

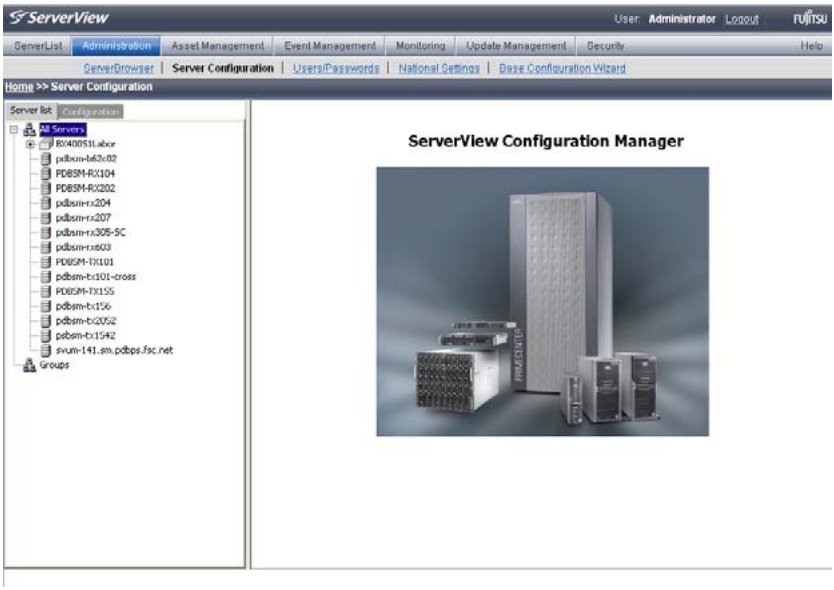



Bild 251: Operations Manager: Fenster „Server Configuration“ - Registerkarte „Server list“ (1)

► Klicken Sie im Strukturbaum der Registerkarte *Server list* auf den zu konfigurierenden Server.

Das folgende Fenster wird angezeigt:

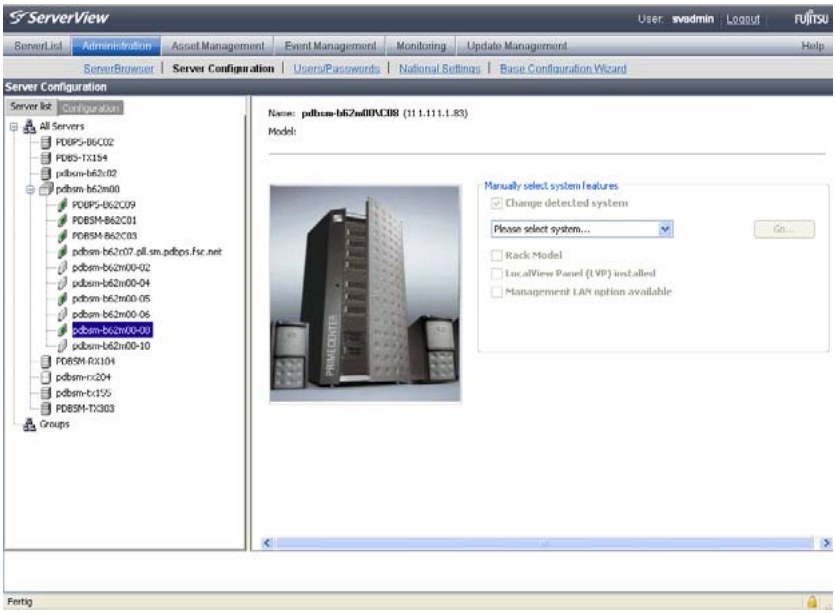



Bild 252: Operations Manager: Fenster „Server Configuration“ - Registerkarte „Server list“ (2)

► Legen Sie im rechten Bereich des Fensters die Details zum gewählten Server fest und klicken Sie auf *GO*.... .

Der erste Dialog des Server Configuration Managers wird angezeigt.

# 10 Firmware aktualisieren

Dieses Kapitel informiert über folgende Themen:

– Firmware des iRMC S4 (Überblick)

– Memory-Stick für die Firmware-Aktualisierung erstellen

– Firmware-Images aktualisieren

– Emergency Flash

– Flash-Tools

**ACHTUNG!**

Beachten Sie beim Aktualisieren / Zurücksetzen der Firmware, dass ein einwandfreies Funktionieren der Firmware nur dann gewährleistet ist, wenn Runtime Firmware und SDR (Sensor Data Record) demselben Firmware-Release angehören.

Die aktuellen Firmware-Versionen erhalten Sie auf der *ServerView Suite DVD 2* oder per manuellem Download aus der Download-Section des Webservers von Fujitsu Technology Solutions.

Die *ServerView Suite DVD 2* können Sie alle zwei Monate aktuell beziehen.

Neben der Firmware-Aktualierung besteht auch die Möglichkeit zum Firmware-Downgrade, d.h. Sie können die Firmware auf den Vorgängerstand zurücksetzen.

Bevor Sie die Firmware aktualisieren oder zurücksetzen, lesen Sie sorgfältig die mit der entsprechenden Firmware gelieferte zusätzliche Dokumentation (vor allem die Readme-Dateien).

# 10.1 Firmware des iRMC S4 (Überblick)

Der iRMC S4 arbeitet mit zwei verschiedenen Firmware-Images. Die beiden Firmware-Images sind jeweils auf EEPROM (**E**lectrically **E**rasable **P**rogrammable **R**ead-**O**nly **M**emory) mit 32 MB gespeichert:

– Firmware-Image 1 (Unteres FW Image, Low FW Image)
– Firmware-Image 2 (Oberes FW Image, High FW Image)

Die Firmware des iRMC S4 wird nicht im EEPROM ausgeführt, sondern wird beim Start in den SRAM-Speicher geladen und dort ausgeführt. Somit können Sie sowohl das aktive als auch das inaktive Firmware-Image online, d.h. bei laufendem Server-Betriebssystem (Windows oder Linux) aktualisieren.

Wenn beim Start der Firmware aus einem der Images ein Fehler erkannt wird, wird die Firmware automatisch aus dem anderen Image gestartet.

Aktuelle Informationen zu Firmware und EEPROM des iRMC S4 erhalten Sie

– an der iRMC S4-Weboberfläche, Seite i*iRMC S4 Information* (siehe Seite 190) oder
– mithilfe der Flash-Tools (siehe Seite 435).

### Aktives und passives Firmware-Image

Jeweils eines der beiden Firmware-Images ist aktiv (running), während das andere inaktiv ist. Welches Firmware-Image aktiv ist, wird über den so genannten Firmware-Selektor festgelegt (siehe Seite 423).

### Firmware-Selektor

Der Firmware-Selektor spezifiziert die Firmware des iRMC S4, die ausgeführt wird. Nach jedem Reset und Neustart des iRMC S4 wird der Firmware-Selektor ausgewertet und es wird auf die entsprechende Firmware verzweigt.

Der Firmware-Selektor kann folgende Werte annehmen:

0 Firmware-Image mit der neuesten Firmware-Version

1 Firmware-Image 1

2 Firmware-Image 2

3 Firmware-Image mit dem ältesten Firmware-Version

4 Firmware-Image, das zuletzt aktualisiert wurde

5 Firmware-Image, das am längsten nicht mehr aktualisiert wurde

Je nach verwendeter Update-Variante ist der Firmware-Selektor nach erfolgtem Update unterschiedlich gesetzt.

Den Firmware-Selektor können Sie abfragen und explizit setzen

– auf der Seite *iRMC S4 Information* der iRMC S4-Weboberfläche (siehe "Aktive Firmware" auf Seite 192)

oder

– mithilfe der Flash-Tools (siehe Seite 435).

## 10.2 USB Memory Stick erstellen

Den USB Memory Stick benötigen Sie **nicht**, wenn Sie die Firmware des iRMC S4 auf einem der folgenden Wege aktualisieren:

- mithilfe des ServerView Update Managers
- mithilfe des ServerView Update Manager Express oder via ASP
- via iRMC S4-Weboberfläche und TFTP-Server

**Gehen Sie wie folgt vor:**

- Laden Sie die Firmware *Firmware Update for USB Stick* aus der Download-Section des Webservers von Fujitsu Technology Solutions in ein Verzeichnis auf Ihrem Rechner.

  In Ihrem Download-Verzeichnis finden Sie das ZIP-Archiv *FTS_<spec>.zip*. (Der Namensbestandteil *<spec>* enthält Informationen zu Systemtyp, Systembaugruppe, Firmware/SDRR-Version etc.):

  Das Zip-Archiv enthält folgende Dateien:

  - *USBImage.exe*
  - *iRMC_<Firmware-Version>.exe*
  - *iRMC_<Firmware-Version>.IMA*

- Verbinden Sie den USB Memory Stick mit Ihrem Rechner.
- Starten Sie die Datei *iRMC_<Firmware-Version>.exe* oder die Datei *USBImage.exe*.

  Je nachdem, welche Datei Sie aufrufen, wird eines der folgenden Fenster geöffnet (siehe Bild 253 auf Seite 425):

Bild 253: Image-Datei auf USB Memory Stick kopieren (mit iRMC_<Firmware version>.exe)

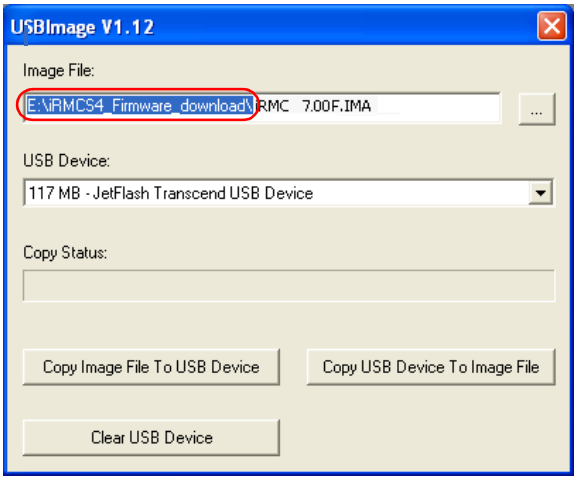



Bild 254: Image-Datei auf USB Memory Stick kopieren (USBImage.exe)

Wenn Sie *USBImag.exe* aufgerufen haben, müssen Sie unter *Image File:* die Datei *iRMC_<Firmware-Version>.IMA* explizit angeben.

► Klicken Sie auf *Clear USB Device*, um die Daten auf dem USB Memory Stick zu löschen.

- Klicken Sie auf *Copy Image File to USB Device*, um die Datei *BMC_<Firmware-Version>.IMA* auf den USB Memory Stick zu kopieren und zu extrahieren.

  **ACHTUNG!**

  Durch diese Aktion wird der Inhalt des USB Memory Sticks überschrieben!

Nach Abschluss des Kopiervorgangs befinden sich Flash-Tools und Image-Dateien auf dem USB Memory Stick:

| Name | Size | Type | Date Modified |
|---|---|---|---|
| FDOS | | Dateiordner | 26.09.2012 10:26 |
| MENU | | Dateiordner | 26.09.2012 10:26 |
| 700F_317.bin | 30.720 KB | BIN-Datei | 29.07.2013 11:43 |
| Autoexec.bat | 1 KB | Stapelverarbeitung... | 09.11.2007 15:02 |
| CHECK.EXE | 15 KB | Anwendung | 19.05.2009 10:44 |
| clibmc.bat | 1 KB | Stapelverarbeitung... | 08.03.2006 10:46 |
| command.com | 65 KB | Anwendung für MS-... | 16.02.2007 13:29 |
| config.sys | 1 KB | Systemdatei | 16.02.2007 14:40 |
| CVT100.EXE | 20 KB | Anwendung | 06.08.1988 20:17 |
| CVT100.SET | 1 KB | SET-Datei | 05.12.2002 15:06 |
| DosYafuf.exe | 183 KB | Anwendung | 22.07.2013 08:01 |
| flashm.bat | 6 KB | Stapelverarbeitung... | 29.07.2013 11:42 |
| FLIRMCS4.EXE | 42 KB | Anwendung | 17.07.2013 09:08 |
| IPMIVIEW.EXE | 148 KB | Anwendung | 03.05.2013 10:59 |
| IPMIVIEW.INI | 14 KB | Konfigurationseinst... | 03.08.2010 14:20 |
| KERNEL.SYS | 45 KB | Systemdatei | 16.02.2007 15:11 |
| readme.txt | 9 KB | Textdokument | 26.07.2013 08:03 |
| SLEEP.EXE | 9 KB | Anwendung | 25.02.1998 20:17 |
| WBAT.INI | 3 KB | Konfigurationseinst... | 08.06.2004 14:12 |

Bild 255: Image-Dateien und Flash-Tools auf dem USB Memory Stick.

## 10.3 Firmware-Images aktualisieren

Da die Firmware des iRMC S4 im SRAM-Speicher des iRMC S4 ausgeführt wird, können Sie sowohl das aktive als auch das inaktive Firmware-Image online, d.h. bei laufendem Server-Betriebssystem aktualisieren.

Für das Update der Firmware-Images stehen Ihnen folgende Möglichkeiten zur Verfügung:

– via iRMC S4-Weboberfläche

– mithilfe des ServerView Update Managers

– mithilfe des ServerView Update Manager Express oder via ASP

– Update mithilfe der Betriebssystem-Flash-Tools.

Wenn eine neue Version des Bootloaders verfügbar ist, werden beide Firmware-Images automatisch im Rahmen desselben Update-Vorgangs mittels Flash übertragen.

**Firmware auf den Vorgängerstand zurücksetzen (Firmware Downgrade)**

Neben der Firmware-Aktualierung besteht auch die Möglichkeit zum Firmware-Downgrade, d.h. Sie können die Firmware auf den Vorgängerstand zurücksetzen.

Als einfachste Möglichkeit für ein Downgrade bietet es sich an, das Firmware-Image der Vorgängerversion als inaktives Firmware-Image im EEPROM des iRMC S4 in Reserve zu halten. Bei Bedarf setzen Sie den Firmware-Selektor auf das Firmware-Image der Vorgängerversion und starten anschließend den iRMC S4 neu, um die Firmware zu aktivieren.

Darüber hinaus können Sie für den Firmware-Downgrade auch die in den folgenden Abschnitten vorgestellten Verfahren einsetzen, indem Sie den Update mit der Firmware der Vorgängerversion durchführen. Führen Sie in diesen Fällen ein Firmware-Update basierend auf der Firmware der vorherigen Version durch. Falls für das Downgrade Besonderheiten zu beachten sind, wird im Folgenden an den entsprechenden Stellen gesondert darauf hingewiesen.

### 10.3.1 Update über die iRMC S4-Weboberfläche

Über die Seite *iRMC S4 Firmware Aktualisierung* können Sie die Firmware des iRMC S4 aktualisieren, indem Sie das gewünschte Firmware-Image wahlweise lokal auf der Remote-Workstation, auf einem Netzlaufwerk oder auf einem TFTP-Server zur Verfügung stellen (siehe Abschnitt "iRMC S4 Firmware Aktualisierung" auf Seite 209).

### 10.3.2 Update via ServerView Update Manager

Mithilfe des ServerView Update Managers können Sie das Update der iRMC S4-Firmware über eine grafische Benutzeroberfläche (Windows) oder über ein Command Line Interface (Windows und Linux) starten. Der ServerView Update Manager greift auf die Update-Daten über sein Update-Repository auf der *ServerView Suite DVD 2* oder dem Management-Server zu. Das Update-Repository auf dem Management-Server aktualisieren Sie mittels Download-Manager oder manuellem Download aus der Download Section des Webservers von Fujitsu Technology Solutions.

Näheres zum Firmware-Update mit dem ServerView Update Manager finden Sie im Handbuch „ ServerView Update Manager“.

### 10.3.3 Online-Update via ServerView Update Manager Express oder ASP

Unter Windows- und Linux-Betriebssystemen können Sie die iRMC S4-Firmware wahlweise mithilfe der grafischen Benutzeroberfläche des ServerView Update Manager Express aktualisieren oder die Kommandoschnittstelle der ASPs (Autonomous Support Package) verwenden.

Unter Windows können Sie ein ASP außerdem im Windows-Explorer per Doppelklick auf die entsprechende ASP-*.*exe*-Datei starten.

**Beachten Sie beim Firmware-Downgrade:**

– Beim Downgrade via Update Manager Express:

  Das Firmware-Downgrade kann nur im *Expert*-Modus durchgeführt werden. Außerdem muss die Option *Downgrade* aktiviert sein.

– Bei Downgrade via ASP:

  – Unter Windows:

    Downgrade ist möglich, wenn Sie das ASP per Doppelklick auf die entsprechende ASP-*.*exe*-Datei starten. Falls sie das ASP über die Kommandoschnittstelle (CLI) starten, müssen Sie die Option *Force=yes* explizit angeben.

  – Unter Linux:

    Sie müssen die Option *-f* bzw. *--force* explizit angeben.

Näheres zum Firmware-Update via Update Manager Express und ASP finden Sie im Handbuch „Lokaler System-Update von PRIMERGY Servern“.

## 10.3.4 Update mit den Betriebssystem-Flash-Tools

Ein Update mithilfe der Betriebssystem-Flash-Tools wird nur als Recovery Flash durchgeführt, d.h. es erfolgt keine Versionsprüfung.

**Voraussetzung:**

Die Flash-Tools sowie die Dateien für den Fimware-Update müssen im Dateisystem des verwalteten Servers vorhanden sein.

Abhängig vom eingesetzten Betriebssystem verwenden Sie eines der folgenden Flash-Tools:

| | |
|---|---|
| DOS: | flirmcs4 |
| Windows: | winflirmcs4<br><br>**Voraussetzung:**<br>Auf dem verwalteten Server müssen die ServerView Agents für die verwendete Windows-Variante (32/64 bit) gestartet sein. |
| Windows (32 bit): | w32flirmcs4 (Agenten sind nicht erforderlich.) |
| Windows (64 bit): | w64flirmcs4 (Agenten sind nicht erforderlich.) |
| Linux: | linflirmcs4 |

Die Flash-Tools rufen Sie in der Windows-Eingabeaufforderung (flirmcs4, w32flirmcs4, w64flirmcs4, winflirmcs4) bzw. am Linux-CLI (linflirmcs4) auf.

Syntax und Operanden der Flash-Tools sind beschrieben im Abschnitt "Flash-Tools" auf Seite 435.

**Gehen Sie wie folgt vor:**

Nachfolgend ist der Online-Update unter Verwendung eines USB Memory Sticks beschrieben (siehe Abschnitt "USB Memory Stick erstellen" auf Seite 424).

- Verbinden Sie den USB Memory Stick mit dem verwalteten Server.
- Wechseln Sie in der Windows-Eingabeaufforderung oder im Command Line Interface (CLI) von Linux zum Laufwerk des USB Memory Sticks.
- Setzen Sie den Firmware-Selektor auf den Wert 4, indem Sie das Flash-Tool mit dem Parameter */s 4* aufrufen

  Geben Sie z.B. in der Windows-Eingabeaufforderung an:

  `w32flirmcs4 /b 4` oder `w64flirmcs4 /b 4`

- Starten Sie den Update der Firmware und der SDR-Daten, indem Sie das Flash-Tool mit den entsprechenden Update-Dateien aufrufen.

  Geben Sie z.B. in der Windows-Eingabeaufforderung an:

  `w32flirmcs4 *.bin /i` oder `w64flirmcs4 *.bin /i`

  Damit wird die neue Version per Flash-Verfahren in den inaktiven EEPROM übermittelt.

  Firmware und SDR werden aus derselben **.bin*-Datei mittels Flash übermittelt.

  Wenn Sie das Flash-Tool mit dem Parameter */wr* aufrufen, wird die aktualisierte Firmware automatisch aktiviert, sobald der Flash-Vorgang abgeschlossen ist. In diesem Fall müssen Sie iRMC S4 nicht neu starten.

  Während des Firmware-Updates werden Sie an der Konsole über den Verlauf des Update-Vorgangs informiert. Im Fehlerfall wird der Update-Vorgang abgebrochen und ein entsprechender Returncode gemeldet (siehe Seite 437).

- Starten Sie den verwalteten Server neu. Das Firmware-Image mit der aktualisierten Firmware wird dadurch automatisch aktiviert.

## 10.3.5 Update über das Menü der FlashDisk

Für den Update über das Menü der FlashDisk benötigen Sie einen bootfähigen USB Memory Stick (siehe Abschnitt "USB Memory Stick erstellen" auf Seite 424).

**Gehen Sie wie folgt vor:**

- Verbinden Sie den USB Memory Stick mit dem verwalteten Server (direkt oder via Remote Storage).
- Booten Sie vom USB Memory Stick.

Nach Abschluss des Bootvorgangs werden die Daten des USB Memory Sticks automatisch in eine RAM Disk kopiert. Anschließend wird die Datei *autoexec.bat* automatisch gestartet.

Das FlashDisk-Menü wird geöffnet:

Bild 256: Menü der FlashDisk

Ein Firmware-Downgrade ist nur via Recovery Flash möglich.

*Normal*

Es wird ein *normal flash* durchgeführt.

Bei einem Normal Flash werden die Bereiche des EEPROM auf Aktualität überprüft, die die aktive Firmware enthalten. If one of these areas is not up to date then the corresponding area for the inactive firmware is updated if it is not already up to date.

*Recovery _L*

Es wird ein *Recovery Flash* für das Firmware-Image 1 (untere Firmware-Image) durchgeführt.

Bei einem Recovery Flash wird der Flash ohne Versionsprüfung für alle drei Bereiche des Firmware-Image 1 durchgeführt.

*Recovery _U*

Es wird ein *Recovery Flash* für das Firmware-Image 2 (oberes Firmware-Image) durchgeführt.

Bei einem Recovery Flash wird der Flash ohne Versionsprüfung für alle drei Bereiche des Firmware-Image 2 durchgeführt.

*Initial*

Sowohl die aktive als auch die inaktive Firmware wird mittels Flash übermittelt.

*Readme*

Die Readme-Datei mit wird angezeigt.

*Reboot*

Es wird ein Warmstart des iRMC S4 durchgeführt.

*English* / *German*

Tastatur-Layout festlegen. Standardmäßig ist *German* eingestellt.

- ► Starten Sie die gewünschte Update-Variante durch Anklicken der entsprechenden Schaltfläche.

  Während des Firmware-Updates werden Sie an der Konsole über den Verlauf des Update-Vorgangs informiert. Im Fehlerfall wird der Update-Vorgang abgebrochen. Ein entsprechender Returncode wird gemeldet (siehe Seite 437).

- ► Klicken Sie nach Abschluss des Update-Vorgangs auf *Exit*, um das FlashDisk-Menü zu verlassen.
- ► Trennen Sie den USB Memory Stick vom verwalteten Server.
- ► Starten Sie den verwalteten Server neu (z.B. mit Ctrl + Alt + Del).

## 10.4 Emergency Flash

Wenn die Firmware des iRMC S4 nicht mehr ausgeführt werden kann, z. B. weil die SDRs nicht mit dem System kompatibel sind, können Sie über den Emergency Mode die Firmware wieder zum Laufen bringen. Im Emergency Mode verzweigt das System automatisch zum Bootloader und ist dann bereit für den Firmware-Update.

Der Emergency Mode wird durch abwechselndes Blinken von Fehler-LED (Global Error LED) (rot) und Identifizierungs-LED (blau) angezeigt.

Um den verwalteten Server in den Emergency Mode zu versetzen und anschließend die Firmware des iRMC S4 zu aktualisieren, verfahren Sie wie folgt:

- Ziehen Sie den Netzstecker.
- Stecken Sie den Stecker bei gedrückter Identify-Taste wieder in die Steckdose.

  Der verwaltete Server befindet sich nun im Emergency Mode.
- Booten Sie den Server nach DOS und aktualisieren Sie die Firmware des iRMC S4 per Recovery Flash.

  Wenn die Firmware nicht aktiv ist, startet der Bootvorgang mit einer zeitlichen Verzögerung von bis zu 2 Minuten. Die Fehlermeldung „iRMC S4 Controller Error“, die das BIOS während dieser Zeit ausgibt, können Sie ignorieren.

## 10.5 Flash-Tools

flirmcs4, w64flirmcs4 und linflirmcs4 w32flirmcs4 unterscheiden sich nur im Namen sowie in der Umgebung, in der sie aufgerufen werden. Die nachfolgende Beschreibung gilt somit auch für diese Tools. Anstelle von „w32flirmcs4“ müssen Sie dabei jeweils „flirmcs4“, „w64flirmcs4“ oder „linflirmcs4“ eingeben.

### Syntax

```
w32flirmcs4 <Dateiname> [<Option>]...
```

<Dateiname> ohne Flash-Optionen: Firmware aktualisieren (wie /u)

### Optionen

/h oder /? Diese Hilfeinformationen anzeigen

/v Tatsächliche Programmversion von „w32flirmcs4“ anzeigen

/vNoDriverLoad Tatsächliche Programmversion von „w32flirmcs4“ anzeigen

/o Tatsächliche Versionen der Firmware anzeigen

/1 Ersten EEPROM mit Versionsprüfung per Flash übermitteln

/2 Zweiten EEPROM mit Versionsprüfung per Flash übermitteln

/f1 Flash-Übermittlung von erstem EEPROM ohne Versionsprüfung erzwingen

/f2 Flash-Übermittlung von zweitem EEPROM ohne Versionsprüfung erzwingen

/fi Flash-Übermittlung von inaktivem EEPROM ohne Versionsprüfung erzwingen

/i Inaktiven EEPROM mit Versionsprüfung per Flash übermitteln

/u Inaktiven EEPROM per Flash übermitteln, wenn neue Version größer als aktives EEPROM ist

/wr Warm Reset der Firmware initiieren

/s [0-2] FW-Upload-Auswahl anzeigen/festlegen

0: Autom. inaktives Images

1: Image 1, unteres Firmware-Image

2: Image 2, oberes Firmware-Image

/b [0-5] FW-Boot-Auswahl anzeigen/festlegen

0: Autom. höhere Firmware-Version auswählen

1: Image 1, unteres Firmware-Image

2: Image 2, oberes Firmware-Image

3: Autom. niedrigere Firmware-Version auswählen

4: Autom. zuletzt programmierte Firmware auswählen

5: Autom. älteste programmierte Firmware auswählen

/n Keine Konsolenausgabe, keine Benutzereingabe erforderlich

/noUserEntry Keine Benutzereingabe erforderlich, aber mit Konsolenausgabe

/logError[file] Fehler in Protokolldatei schreiben, Standard: w32flirmcs4.logError

/logOutput[file] Jede Terminal-Ausgabe in Protokolldatei schreiben,

Standard: w32flirmcs4.logOutput

/logOutput[file] Jede interne Debug-Ausgabe in Protokolldatei schreiben,

Standard: w32flirmcs4.logDebug

/ignore Ausgewähltes EEPROM ohne Prüfung mittels Flash übertragen (FW-Version, SDR ID)

/d [0-99] [0-99] Zusätzliche Debug-Ausgabe [Verbose-Level]

a) ohne Verbose-Level: gesamte Debug-Ausgabe drucken

b) ein Verbose-Level: Debug-Ausgabe drucken <= Verbose-Level

c) zwei Verbose-Level: Debug-Ausgabe zwischen

1. und 2. Verbose-Level drucken

/e Emulationstestmodus (kein Zugriff auf iRMC, nur zu Testzwecken)

/noExitOnError Kein Programm zum Beenden und Fortfahren nach Fehler (nur zu Testzwecken)

99: Kein Flash, da EEPROM-Firmware aktuell ist

## Returncodes

| Wert | Bedeutung |
|---|---|
| 00 | Kein Fehler, Programm erfolgreich abgeschlossen. |
| 01 | Argumente fehlen oder sind fehlerhaft. |
| 02 | Firmware-Upload-Auswahlwert außerhalb des Bereichs (0-2). |
| 03 | Firmware-Boot-Auswahlwert außerhalb des Bereichs (0-5). |
| 04 | Firmware-Image-File fehlt. |
| 05 | Firmware-Image-File konnte nicht geöffnet werden. |
| 06 | Kommunikation mit BMC nicht möglich. |
| 07 | Falscher Abschlusscode des IPMI-Kommandos. |
| 08 | Das System hat kein iRMC S4. |
| 09 | SDR-ID des System und Flash-Image-File stimmen nicht überein. |
| 10 | Speicherpuffer kann nicht zugewiesen werden. |
| 11 | Dateiübertragung fehlgeschlagen. |
| 12 | IPMI-Aufruf fehlgeschlagen (Reaktionsdatengröße ist 0). |
| 13 | HTI-Schnittstelle ist nicht verfügbar. |
| 14 | HTI-Schnittstellenerkennung fehlgeschlagen (anderer Erkennungsfehler). |
| 15 | HTI-Schnittstellenerkennung fehlgeschlagen (ScSBB2.sys-Treiber nicht verfügbar). |
| 16 | Verbindung mit HTI fehlgeschlagen. |
| 17 | Flash-Prozess fehlgeschlagen. |
| 18 | Fehlerabschlusscode von [F5 0B Start TFTP Flash]: 0xCB.<br>Keine Daten vorhanden (TFTP-Server konnte das angeforderte Image-File nicht bereitstellen) |
| 19 | Fehlerabschlusscode von [F5 0B Start TFTP Flash]: 0xD3.<br>Ziel nicht verfügbar (TFTP-Server kann nicht erreicht werden). |
| 20 | Unbekannter Abschlusscode von [F5 0B Start TFTP Flash]: |
| 21 | Falsche Dateigröße des Firmware-Image-Files. |
| 22 | Fehler in Firmware-Image-File. |
| 23 | GetFullPathName fehlgeschlagen. |
| 24 | Image kann nicht geladen werden, da Flash-Status 0x04 ist (Image-Download läuft). |
| 25 | Image kann nicht geladen werden, da Flash-Status 0x08 ist (Flash läuft). |
| 26 | Unerwarteter Flash-Status des iRMC vor Laden der Datei. |

Tabelle 24: Returncodes der Flash-Tools

| Wert | Bedeutung |
|---|---|
| 27 | Firmware-Image-File existiert nicht. |
| 28 | Unerwartete IPMI-Kommando-Reaktionsdatengröße. |
| 29 | Unerwarteter Rückgabewert von HTI-Funktion. |
| 30 | Das Betriebssystem kann dieses Anwendungsprogramm nicht ausführen. |

Tabelle 24: Returncodes der Flash-Tools

# 11 Remote-Installation des Betriebssystems via iRMC S4

Dieses Kapitel bietet einen Überblick darüber, wie Sie mithilfe des ServerView Installation Managers (im Folgenden kurz Installation Manager genannt) sowie mittels der iRMC S4-Funktionen „Grafische Konsolen Umleitung“ (AVR, Advanced Video Redirection) und „Remote Storage“ von der Remote-Workstation aus das Betriebssystem auf dem verwalteten Server installieren.

Im Einzelnen informiert das Kapitel über folgende Themen:

– Allgemeines Vorgehen bei der Remote-Installation eines Betriebssystems mithilfe von Remote Storage-Speichermedien, die mithilfe der Funktion „Virtuelle Medien“ bereitgestellt werden. Im Folgenden werde die mit der Funktion „Virtuelle Medien“ bereitgestellten Speichermedien kurz virtuelle Speichermedien genannte.

– Verwalteten Server von der Remote-Workstation aus über die ServerView Suite DVD 1 booten (Windows und Linux).

– Windows nach Konfiguration auf dem verwalteten Server von der Remote-Workstation aus installieren.

– Linux nach Konfiguration auf dem verwalteten Server vom Remote-Arbeitsplatz aus installieren.

Die Beschreibung legt den Schwerpunkt auf den Umgang mit virtuellen Speichermedien. Kenntnisse der Funktionalität des Installation Managers werden vorausgesetzt (siehe Handbuch „ServerView Installation Manager“).

**Voraussetzungen für eine Remote-Installation des Betriebssystems via iRMC S4:**

– Die LAN-Schnittstelle des iRMC S4 muss konfiguriert sein (siehe Seite 45)

– Der Lizenzschlüssel (License Key) für die Nutzung der iRMC S4-Funktionen „Grafische Konsolen-Umleitung“ und „Virtual Media“ muss installiert sein (siehe Seite 193).

# 11.1 Betriebssystem via iRMC S4 installieren - generelles Vorgehen

Die Remote-Installation des Betriebssystems via iRMC S4 ist aus Sicht des Installation Managers eine lokale Konfiguration und Installation des Betriebssystems auf dem verwalteten Server, die Sie von der Remote-Workstation aus über das AVR-Fenster mithilfe von virtuellen Speichermedien durchführen.

Im Einzelnen sind für eine Installation mittels Installation Manager folgende Schritte erforderlich:

1. Virtuelles Speichermedium (DVD oder Installation Manager Boot-Image), von dem gebootet werden soll, als virtuelles Speichermedium verbinden.
2. Verwalteten Server über die DVD oder das Installation Manager Boot-Image booten und konfigurieren.
3. Betriebssystem via Installation Manager von der Remote-Workstation aus auf dem verwalteten Server installieren.

**Windows ohne Installation Manager mithilfe der Windows-Installations-CD/DVDs installieren**

Die Remote-Installation von Windows via Virtuelle Medien können Sie wahlweise mithilfe des Installation Managers oder ausschließlich mithilfe der Windows-Installations-CD/DVDs durchführen. Hinsichtlich des Umgangs mit den virtuellen Speichermedien stimmen beide Verfahren überein.

Aus folgenden Gründen empfiehlt sich jedoch eine Windows-Installation mithilfe des Installation Managers:

– Der Installation Manager ermittelt selbstständig die erforderlichen Treiber und kopiert diese in das System.

– Während der Installation stehen Ihnen alle Installation Manager-Funktionen zur Verfügung So können Sie z.B. das gesamte System inklusive der Einstellungen für das Server-Management konfigurieren.

– Die Installation ohne Installation Manager müssen Sie über die Tastatur steuern, da während des Installationsvorgangs der Mauszeiger nicht synchronisiert werden kann. Dagegen können Sie bei der Installation via Installation Manager die gesamte Konfiguration und Installation mithilfe der Maus abwickeln.

– Bei der Installation ohne Installation Manager müssen Sie alle erforderlichen Einstellungen für die Synchronisation des Mauszeigers nachträglich „von Hand“ durchführen.

– Die Installation via Installation Manager dauert nicht wesentlich länger als die Installation mithilfe der Betriebssystem-CD/DVDs.

**Linux ohne Installation Manager mithilfe der Linux-Installations-CD/DVD installieren**

Wenn Sie die vom System benötigten Treiber kennen, können Sie die Linux-Installation auch durch Booten von der Linux-Installations CD/DVD starten.

Falls die Installation eine Treiber-Integration von der Floppy-Disk erfordert, müssen Sie vor Beginn der Installation jeweils eine virtuelle Medien-Verbindung einrichten

– zum Speichermedium (CD-ROM/DVD-ROM oder ISO Image), von dem aus gebootet werden soll, sowie

– ggf. Speichermedium für die Treiber-Installation.

## 11.2 Speichermedium als Virtual Media verbinden

Die Funktion „Virtuelle Medien“ stellt dem verwalteten Server ein „virtuelles“ Laufwerk zur Verfügung, das sich an anderer Stelle im Netzwerk befindet.

Die Source für das virtuelle Laufwerk kann sein:

– Physisches Laufwerk oder Image-File am Remote-Arbeitsplatz. Das Image-File kann außerdem auf einem Netzlaufwerk liegen (mit Laufwerksbuchstaben, z. B. „D:“ für Laufwerk D).

– Image-File, die zentral über „Dezentrale Medien Abbilder verbinden“ im Netzwerk bereitgestellt wird.

Ausführliche Informationen zur Funktion „Virtuelle Medien“ finden Sie unter Kapitel "Virtuelle Medien Wizard" auf Seite 123.

**Speichermedium am Remote-Arbeitsplatz als virtuellen Storage verbinden**

Gehen Sie folgendermaßen vor, um eine virtuelle Medien-Verbindung an der Remote-Workstation herzustellen:

► Melden Sie sich mit „Remote Storage Enabled“-Berechtigung an der iRMC S4-Weboberfläche an.

► Öffnen Sie die Seite *Grafische Konsolen-Umleitung (AVR)* und starten Sie die AVR .

► Starten Sie im AVR-Fenster „Virtuelle Medien“

► Bereiten Sie die Speichermedien als virtuelle Speichermeiden vor:

– Bei Installation via Installation Manager:

  ServerView Suite DVD 1 oder Installation Manager Boot-Image sowie optional einen formatierten USB Memory Stick als Status-Backup-Medium

– Bei Installation von der Installations-CD/DVD des Herstellers: Windows oder Linux Installations-CD/DVD und optionale Treiber

Es wird empfohlen, die ServerView Suite DVD 1 bzw. die Betriebssystem-Installations-CD/DVD als Image-File (ISO Image) in einem Verzeichnis zu speichern und von dort als virtuelles Speichermedium zu verbinden oder via Remote Image Mount zur Verfügung zu stellen.

Die vorbereiteten Speichermedien werden im Dialogfenster *Virtuelle Medien* angezeigt.

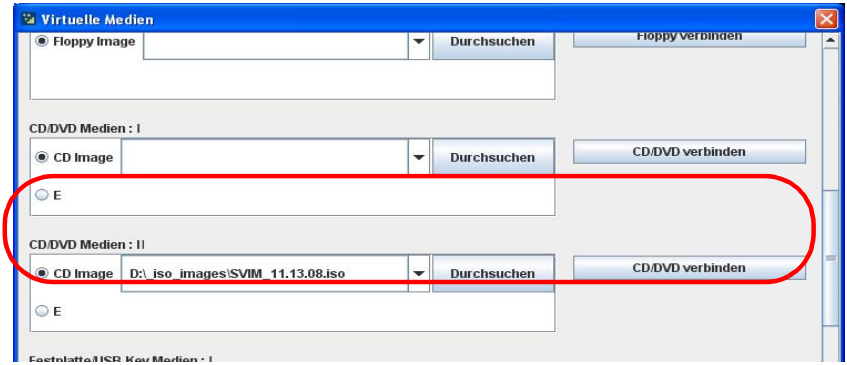



Bild 257: Dialogfenster „Storage Devices“: ServerView Suite DVD ISO-Image

- Klicken Sie auf *Connect*, um das DVD-ROM-Laufwerk (DVD) oder das Installation Manager Boot-Image als virtuelles Speichermedium zu verbinden.

### Über Remote Image Mount bereitgestelltes ISO-Image (Image-File) verbinden

Eine via Remote Image Mount bereitgestelltes Image-File können Sie zum Booten von einem Installation Manager Boot-Image verwenden.

Informationen zum Bereitstellen einer Image-File über Remote Image Mount finden Sie unter Abschnitt "Speichermedium als Virtual Media verbinden" auf Seite 442:

## 11.3 Verwalteten Server von der ServerView Suite DVD 1 booten und via Installation Manager konfigurieren

Gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- ► Schalten Sie über die iRMC S4-Weboberfläche den verwalteten Server ein oder starten Sie den Server neu. Den Bootvorgang können Sie im AVR-Fenster verfolgen.

  Während der BIOS POST-Phase des verwalteten Servers werden virtuelle Speichermedien als USB 2.0-Geräte angezeigt. Virtuelle Speichermedien werden durch die folgenden Einträge in der Boot-Sequenz des BIOS repräsentiert:

  – Eine (physische) Floppy-Disk wird durch einen eigenen Eintrag „FTS RemoteStorage FD-(USB 2.0)“ repräsentiert.

  – Alle anderen virtuellen Storage-Geräte-Typen werden durch einen gemeinsamen Eintrag „CD-ROM DRIVE“ repräsentiert.

  > **i** Wenn am verwalteten Server gleichzeitig ein lokales CD-ROM/DVD-ROM-Laufwerk und ein als virtuelles Medium verbundenes CD-ROM/DVD-ROM-Laufwerk angeschlossen sind, bootet der verwaltete Server von dem über das virtuelle Image bereitgestellten CD-ROM/DVD-ROM-Laufwerk.

- ► Drücken Sie während des Boot des Servers die Taste F2.
- ► Rufen Sie im UEFI-Setup das Menü *Boot* für die Festlegung der Boot-Sequenz auf.
- ► Legen Sie die Boot-Priorität 1 (höchste Priorität) für die als virtuelles Speichermedium verbundene ServerView Suite DVD 1 fest.
- ► Speichern Sie die Einstellungen und beenden Sie das UEFI Setup.

Danach bootet der verwaltete Server von der als virtuellem Storage verbundenen ServerView Suite DVD 1.

> **i** **Falls das System nicht vom virtuellen Speichermedium (ServerView Suite DVD 1 oder Installation Manager Boot-Image) bootet :**
>
> ► Prüfen Sie, ob das Speichermedium während der BIOS POST-Phase angezeigt wird, und verbinden Sie erforderlichenfalls das Speichermedium als virtuelles Medium.

► Stellen Sie die korrekte Boot-Reihenfolge sicher.

Das Booten von der ServerView Suite DVD 1 über ein virtuelles Speichermedium dauert etwa 5 Minuten. Während des Bootens werden Sie über den Fortschritt des Bootvorgangs informiert. Nach Abschluss des Bootvorgangs fordert Sie eine Dialogbox auf, ein Medium für den Statussicherungsbereich (Status-Backup-Medium) auszuwählen.

► Wählen Sie unter *Installation Manager Modus* den *Standard Modus*.

► Legen Sie fest, ob die Konfigurationsdaten auf einem lokalen Wechseldatenträger oder einem Netzwerkmedium gespeichert werden sollen:

i Beachten Sie: Wenn Sie keine Option zur Statussicherung wählen, gehen sämtliche Konfigurationsdaten bei einem Reboot verloren.

*Medium zur Statussicherung*

i Das Backup-Medium darf nicht schreibgeschützt sein.

Ein USB-Stick muss bereits beim Systemstart am USB-Port angeschlossen sein. Falls dies versäumt wurde und Sie die Konfigurationsdatei abspeichern wollen: Schließen Sie den USB-Stick jetzt an und starten Sie einen Reboot von der ServerView Suite DVD 1.

► Wählen Sie die Option *auf lokalem Laufwerk (Diskette / USB Stick)*.

► Wählen Sie im Auswahlfeld rechts von der Option das entsprechende Laufwerk aus.

Nähere Informationen zur Erzeugung von Installation Manager-Statusdisketten erhalten Sie im Handbuch „ServerView Installation Manager“.

*Statusmedium und/oder Installationsmedien über das Netzwerk anbinden*

► Treffen Sie zu diesem Zweck die erforderlichen Freigaben.

i Wenn Sie ein Medium mit einer vorbereiteten Konfigurationsdatei und/oder ein Installationsmedium via Netz bereitstellen, müssen Sie diese Option wählen. Für die aktuelle Installation Manager-Sitzung können Sie, abhängig von Ihrer Infrastruktur, entweder eine temporäre IP-Adresse via DHCP beziehen oder manuell eine IPv4- oder IPv6-Adresse konfigurieren.

► Starten Sie den Installation Manager durch Klicken auf *Weiter*.

### Lokales Deployment starten

Nach dem Start des Installation Managers wird das Begrüßungsfenster angezeigt:

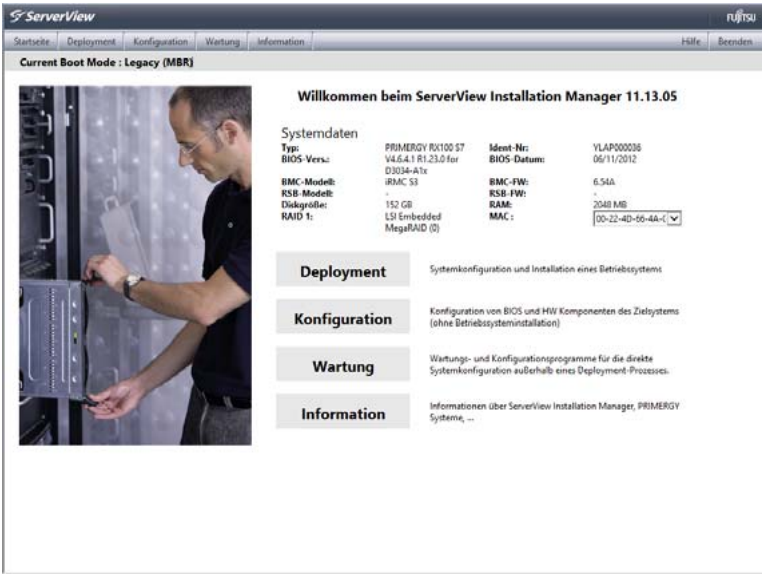



Bild 258: Installation Manager - Begrüßungsfenster

- Klicken Sie auf *Deployment*, um die Vorbereitung der lokalen Installation (Deployment) zu starten.

  Zur Vorbereitung der Installation werden Sie von den Wizards des Installation Managers durch eine Folge von Konfigurationsschritte geführt, in denen Sie die Vorgaben für die Konfiguration des Systems sowie für die anschließende bedienerlose Betriebssystem-Installation zusammenzustellen.

  Konfigurieren Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers. Dann können Sie die Windows Installations-CD/DVD auch über das CD-ROM/DVD-ROM-Laufwerk der Remote-Workstation bereitstellen, wenn Sie dieses als virtuelles Speichermeidum mit dem verwalteten Server verbinden (siehe Abschnitt "Windows nach Konfiguration auf dem verwalteten Server installieren" auf Seite 448).

Nach Abschluss der Konfiguration mit dem Installation Manager wird der Dialog *Installationsparameter* für die Windows-Installation (siehe Seite 448) bzw. für die Linux-Installation (siehe Seite 450) angezeigt, über den Sie den installationsprozess starten können. Dies ermöglicht es Ihnen, den Installationsprozess zu starten.

# 11.4 Betriebssystem nach Konfiguration auf dem verwalteten Server installieren

Im Anschluss an die Konfiguration installieren Sie das Betriebssystem auf dem verwalteten Server.

## 11.4.1 Windows nach Konfiguration auf dem verwalteten Server installieren

Nach Abschluss der Konfiguration zeigt der Installation Manager folgenden Dialog an:

Bild 259: Installation Manager - Installation starten

Wenn Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers konfiguriert haben, gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- ► Trennen Sie Ihre zurzeit aktiven virtuellen Verbindungen.
- ► Entfernen Sie die ServerView Suite DVD 1 aus dem DVD-ROM-Laufwerk am Remote-Arbeitsplatz.
- ► Legen Sie die Windows-Installations-CD/DVD in dieses DVD-ROM-Laufwerk ein.

  Schließen Sie die Anwendung, falls *autostart* aktiviert ist.

- ► Verbinden Sie das CD-ROM/DVD-ROM-Laufwerk, das die Windows-Installations-CD/DVD enthält, als virtuelles Speichermedium.
- ► Klicken Sie auf der Seite *Installationsparameter* des Installation Manager auf *Installation starten*.

  Alle Installationsdateien werden auf den verwalteten Server kopiert.

  In einem Bestätigungsdialog informiert Sie der Installation Manager über den Abschluss des Kopiervorgangs und fordert Sie auf, vor dem automatischen Neustart des verwalteten Servers alle Speichermedien aus den Wechsellaufwerken zu entfernen.

  Insbesondere müssen Sie vor dem Neustart des Systems auch alle aktiven virtuellen Medien-Verbindungen trennen.

- ► Gehen Sie zum Trennen der aktuellen virtuellen Medien-Verbindungen folgendermaßen vor:
  - ► Starten Sie „Virtuelle Medien“.

    Das Dialogfenster *Virtuelle Medien* wird angezeigt und enthält die derzeit verbundenen virtuellen Storage-Geräte.

  - ► Führen Sie ein „Sicheres Trennen“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.
  - ► Klicken Sie auf *Disconnect...*, um alle virtuellen Storage-Verbindungen zu trennen.
- ► Klicken Sie im Bestätigungsdialog auf *Ok*, um den verwalteten Server neu zu starten.

Nach dem Neustart des verwalteten Servers können Sie komplette Installation mithilfe der AVR überwachen.

## 11.4.2 Linux nach Konfiguration auf dem verwalteten Server installieren

Die Maus kann während der Linux-Installation verwendet, aber nicht synchronisiert werden

Bei jedem Wechsel eines virtuellen Speichermediums müssen Sie die virtuelle Medien-Verbindung des aktuell verbundenen Mediums trennen und anschließend das neue Medium als virtuelles Speichermedium verbinden.

Nach Abschluss der Konfiguration zeigt der Installation Manager folgenden Dialog an:

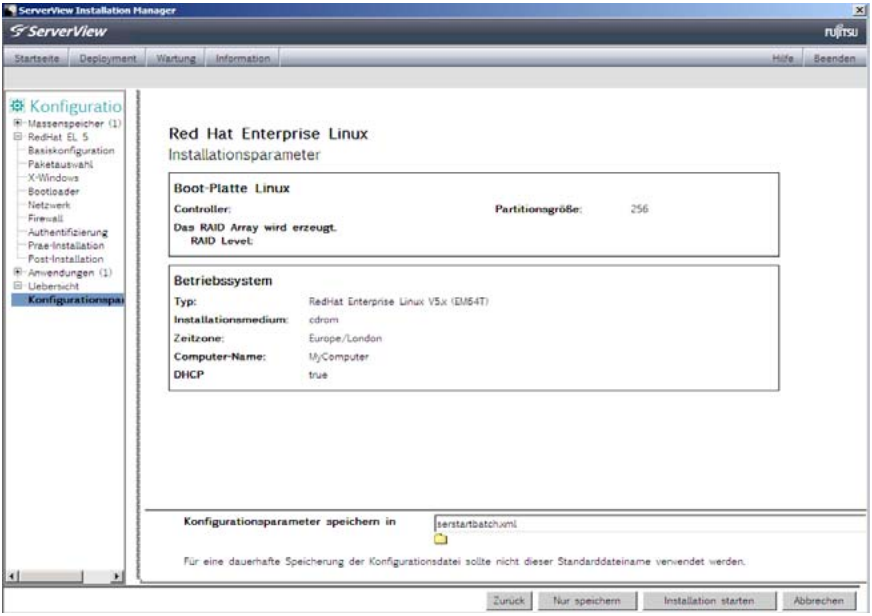



Bild 260: Installation Manager - Installation starten

Wenn Sie als Installationsquelle das lokale CD-ROM/DVD-ROM-Laufwerk des verwalteten Servers konfiguriert haben, gehen Sie am Remote-Arbeitsplatz wie folgt vor:

- ► Trennen Sie Ihre zurzeit aktiven virtuellen Medien-Verbindungen. .
- ► Entfernen Sie die ServerView Suite DVD 1 aus dem DVD-ROM-Laufwerk am Remote-Arbeitsplatz.
- ► Legen Sie die Linux-Installations-CD/DVD in dieses DVD-ROM-Laufwerk ein.

  Schließen Sie die Anwendung, falls *autostart* aktiviert ist.

- ► Verbinden Sie das CD-ROM/DVD-ROM-Laufwerk, das die Linux-Installations-CD/DVD enthält, als virtuelles Speichermedium.
- ► Klicken Sie auf der Seite *Installationsparameter* des Installation Manager auf *Installation starten*.

  Alle Installationsdateien werden auf den verwalteten Server kopiert. In einem Bestätigungsdialog informiert Sie der Installation Manager über den Abschluss des Kopiervorgangs und fordert Sie auf, vor dem automatischen Neustart des verwalteten Servers alle Speichermedien aus den Wechsellaufwerken zu entfernen.

  Insbesondere müssen Sie vor dem Neustart des Systems auch alle aktiven virtuellen Medien-Verbindungen trennen.

- ► Trennen Sie vor dem Neustart des Systems die aktuellen virtuellen Medien-Verbindungen.

  Gehen Sie hierbei wie folgt vor:

  - ► Starten Sie „Virtuelle Medien“.

    Das Dialogfenster *Virtuelle Medien* wird angezeigt und enthält die derzeit verbundenen virtuellen Medien-Geräte.

  - ► Klicken Sie auf *Disconnect...*, um alle virtuellen Medien-Verbindungen zu trennen.
  - ► Führen Sie ein „Sicheres Trennen“ für die angezeigten Speichermedien durch, d.h. stellen Sie sicher, dass keine Anwendungen/Programme mehr auf die Speichermedien zugreifen.

- Klicken Sie im Bestätigungsdialog auf *Ok*, um den verwalteten Server neu zu starten.

Nach dem Neustart des verwalteten Servers können Sie komplette Installation mithilfe der AVR überwachen.

# 12 Anhang

Der Anhang informiert über folgende Themen:


– "Vom iRMC S4 unterstützte IPMI OEM-Kommandos" on page 453

– "iRMC S4 mit SCCI und per Skript-Konfiguration konfigurieren" on page 481


## 12.1 Vom iRMC S4 unterstützte IPMI OEM-Kommandos

Dieser Abschnitt beschreibt eine Auswahl der vom iRMC S4 unterstützten OEM-spezifischen IPMI-Kommandos.

### 12.1.1 Überblick

Folgende IPMI OEM-Kommandos werden vom iRMC S4 unterstützt:

- SCCI-konforme Power On/Off-Kommandos
  (SCCI: **S**erverView **C**ommon **C**ommand **I**nterface)
  - 0115 Get Power On Source
  - 0116 Get Power Off Source
  - 011C Set Power Off Inhibit
  - 011D Get Power Off Inhibit
  - 0120 Set Next Power On Time
- **SCCI-konforme Kommunikationskommandos**
  - 0205 System OS Shutdown Request
  - 0206 System OS Shutdown Request and Reset
  - 0208 Agent Connect Status
  - 0209 Shutdown Request Cancelled
- **SCCI-konforme Signalkommandos**
  - 1002 Write to System Display

- **Firmware-spezifische Kommandos**
  - 2004 Set Firmware Selector
  - 2005 Get Firmware Selector
  - C019 Get Remote Storage Connection
  - C01A Set Video Display on/off
- **BIOS-spezifisches Kommando**
  - F109 Get BIOS POST State
  - F115 Get CPU Info
- **iRMC S4-spezifische Kommandos**
  - F510 Get System Status
  - F512 Get EEPROM Version Info
  - F542 Get HDD lightpath status (Component Status Signal Read)
  - F543 Get SEL entry long text
  - F545 Get SEL entry text
  - F5B0 Set Identify LED
  - F5B1 Get Identify LED
  - F5B3 Get Error LED
  - F5DF Set Nonvolatile Cfg Memory to Default Values
  - F5E0 Set Configuration Space to Default Values
  - F5F8 Delete User ID

## 12.1.2 Beschreibung der IPMI OEM-Kommandos

Nachfolgend sind die OEM-spezifischen IPMI-Kommandos im Einzelnen beschrieben.

### 12.1.2.1 Beschreibungsformat

Die OEM-spezifischen IPMI-Kommandos dieses Kapitels sind in dem Format beschrieben, das der IPMI-Standard für die Beschreibung der IPMI-Kommandos verwendet.

Der IPMI-Standard beschreibt die IPMI-Kommandos in Form von Kommando-Tabellen, in denen die Eingabe- und Ausgabeparameter des betreffenden Kommandos aufgelistet sind.

Informationen zu den IPMI-Standards finden Sie im Internet:

*http://developer.intel.com/design/servers/ipmi/index.htm*

### 12.1.2.2 SCCI-konforme Power On/Off-Kommandos

#### 01 15 - Get Power On Source

Dieses Kommando informiert über die Ursache des zuletzt durchgeführten „Power On“. Die möglichen Ursachen werden nachfolgend aufgeführt.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **01** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **15** Command Specifier |
| Response Data | - | **BC** |
| | - | **01** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 3 | **01** Data Length |
| | 4 | Power on Source: Ursache des letzten Power On |

| Power On Source | Beschreibung |
|---|---|
| 0x00 | Software oder Kommando |
| 0x01 | Netzschalter (auf der Frontseite des Servers oder auf der Tastatur) |
| 0x02 | Automatischer Restart nach Stromausfall |
| 0x03 | Uhr oder Timer (Hardware Real-Time Clock (RTC) oder Software Timer) |
| 0x04 | Automatischer Restart nach Shutdown aufgrund eines Lüfterausfalls |
| 0x05 | Automatischer Restart nach Shutdown aufgrund kritischer Temperatur |
| 0x08 | Reboot nach Watchdog Timeout |
| 0x09 | Einschalten vom Remote-Arbeitsplatz aus (Modem RI Line, SCSI Termination Power, LAN, Chip-Kartenleser usw.) |
| 0x0C | Reboot nach CPU-Fehler |
| 0x15 | Reboot durch Hardware-Reset |
| 0x16 | Reboot nach Warmstart |
| 0x1A | Eingeschaltet durch ein Ereignis (Event) des PCI BUS Power Management |
| 0x1D | Eingeschaltet via Remote Manager vom Remote-Arbeitsplatz aus |
| 0x1E | Reboot/Reset via Remote Manager vom Remote-Arbeitsplatz aus |

### 01 16 - Get Power Off Source

Dieses Kommando informiert über die Ursache des zuletzt durchgeführten „Power Off“. Die möglichen Ursachen werden nachfolgend aufgeführt.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **01** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **16** Command Specifier |
| Response Data | - | **BC** |
| | - | **01** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 3 | **01** Data Length |
| | 4 | Power off Source: Ursache des letzten Power Off |

| Power Off Source | Beschreibung |
|---|---|
| 0x00 | Software (SWOFF, SE: Power OFF per Kommando) |
| 0x01 | Netzschalter (auf der Frontseite des Servers oder auf der Tastatur) |
| 0x02 | Fehlerhafte Stromversorgung |
| 0x03 | Uhr oder Timer (Hardware Real-Time Clock (RTC) oder Software Timer) |
| 0x04 | Lüfterausfall |
| 0x05 | Kritische Temperatur |
| 0x08 | Finales Ausschalten nach wiederholtem Watchdog Timeout |
| 0x0C | Finales Ausschalten nach wiederholtem CPU-Fehler |
| 0x1D | Ausgeschaltet via Remote Manager vom Remote-Arbeitsplatz aus |

### 01 1C - Set Power Off Inhibit

Dieses Kommando setzt das *Power Off Inhibit*-Flag, mit dem ein willkürliches Ausschalten des Servers temporär verhindert werden kann.

Bei gesetztem *Power Off Inhibit*-Flag speichert die Firmware die Ursache für einen willkürlich versuchten "Power Off", "Power Cycle" oder Server-Neustart, führt die entsprechende Aktion jedoch nicht aus. Aktuell gespeichert wird dabei immer die Ursache für den zuletzt initiierten "Power Off"-, "Power Cycle"- oder Neustart-Versuch. Die gespeicherte Aktion wird erst nach dem Rücksetzen des *Power Off Inhibit*-Flags ausgeführt.

Das *Power Off Inhibit*-Flag wird nach einem Stromausfall oder bei Betätigung der Reset-Taste automatisch zurückgesetzt.

In seiner Wirkung entspricht das *Power Off Inhibit*-Flag dem Dump-Flag, das bei Erstellen eines Hauptspeicher-Dumps benutzt wird. Hier muss der Initiator vor dem Ziehen des Dumps das Flag setzen und nach Dump-Erstellung wieder zurücksetzen.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFn\|LUN: OEM/Group |
| | - | **01** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 4 | **1C** Command Specifier |
| | 5 | **00** Object ID |
| | 6:7 | **00 00** Value ID |
| | 8 | **01** Data Length |
| | 9 | Power Off Inhibit-Flag: 0 no Inhibit, 1 Inhibit |
| Response Data | - | **BC** |
| | - | **01** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |

### 01 1D - Get Power Off Inhibit

Dieses Kommando ermittelt den Wert des *Power Off Inhibit*-Flags.

Weitere Informationen zum *Power Off Inhibit*-Flag finden Sie in der Beschreibung zu "01 1C - Set Power Off Inhibit" on page 458.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFn\|LUN: OEM/Group |
| | - | **01** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 4 | **1D** Command Specifier |
| Response Data | - | **BC** |
| | - | **01** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 5 | **01** Response Data Length |
| | 6 | Power Off Inhibit-Flag: 0 no Inhibit, 1 Inhibit |

### 01 20 - Set Next Power On Time

Dieses Kommando veranlasst das Einschalten des Systems zum spezifizierten Zeitpunkt, unabhängig von den im Configuration Space konfigurierten Ein-/Ausschalt-Zeiten.

Das Kommando bewirkt nur ein einmaliges Ausschalten

Eine zuvor per 01 20-Kommando festgelegte "Power On"-Zeit annullieren Sie, indem Sie mit einem nachfolgenden 01 20-Kommando die Power On-Zeit "0" spezifizieren.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **01** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **20** Command Specifier |
| | 5 | **00** Object ID |
| | 6:7 | **00 00** Value ID |
| | 8 | **04** Data Length |
| | 9:12 | Time (LSB first) (siehe unten) |
| Response Data | - | **BC** |
| | - | **01** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

*Time (LSB first)*

Zeitpunkt, dargestellt im UNIX-spezifischen Format, zu dem der Server sich wieder einschalten soll. Die Zeitangabe wird NICHT nicht-flüchtig gespeichert. Die Auflösung beträgt 1 Minute. Nach Einschalten des Servers zum spezifizierten Zeitpunkt wird die Zeitangabe intern auf 0 gesetzt.

Bei Angabe Time == 0 wird der Server nicht eingeschaltet.

#### 12.1.2.3 SCCI-konforme Kommunikationskommandos

Die SCCI-konformen Kommunikationskommandos setzen voraus, dass der Agent-Service unter dem Server-Betriebssystem läuft. Für die Ausführung der Kommandos kommuniziert der iRMC S4 mit dem Agenten, der die Aktion dann ausführt.

**02 05 - System OS Shutdown Request**

Dieses Kommando initiiert den Shutdown des Server-Betriebssystems.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **02** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **05** Command Specifier |
| Response Data | - | **BC** |
| | - | **02** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

**02 06 - System OS Shutdown Request and Reset**

Dieses Kommando initiiert den Shutdown des Server-Betriebssystems und den anschließenden Neustart des Systems.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **02** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **06** Command Specifier |
| Response Data | - | **BC** |
| | - | **02** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

### 02 08 - Agent Connect Status

Dieses Kommando prüft, ob der SCCI-Agent aktiv ist.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **02** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **08** Command Specifier |
| Response Data | - | **BC** |
| | - | **02** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 5 | **01** Data Length |
| | 6 | **Connect Status:**<br>00: Verbindung verloren, keine Verbindung zum Agenten.<br>01: Verbindung wiederhergestellt, Verbindung zum Agenten existiert. |

### 02 09 - Shutdown Request Cancelled

Dieses Kommando annulliert einen aktuellen Shutdown-Request.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **02** Cmd : Command Group Communication |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **09** Command Specifier |
| Response Data | - | **BC** |
| | - | **02** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

#### 12.1.2.4 SCCI-konformes Signalkommando

### 10 02 - Write to System Display

Dieses Kommando gibt Text auf ein angeschlossenes LocalView Display aus.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **10** Cmd : Command Group Fan Test |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **02** Command Specifier |
| | 5 | **Object Index**: : Zeile auf dem Display, in die geschrieben werden soll. |
| | 6:7 | **Value ID** (nicht verwendet) |
| | 8 | **Length** Anzahl der zu schreibenden Zeichen + 1. (Der String braucht nicht durch das NULL-Byte terminiert zu sein. Falls die Länge des Displays für die Darstellung des Strings nicht ausreicht, werden überzählige Zeichen abgeschnitten.) |
| | 9 | **Attribut:**<br>0 = String linksbündig schreiben<br>1 = String zentriert schreiben |
| | 10:10+n | **Zeichen**, die auf das Display geschrieben werden sollen. Der String braucht nicht durch das NULL-Byte terminiert zu sein. |
| Response Data | - | **BC** |
| | - | **10** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

### 12.1.2.5 Firmware-spezifische Kommandos

#### 20 04 - Set Firmware Selector

Dieses Kommando konfiguriert, welches Firmware-Image des iRMC S4 nach einem Firmware-Reset aktiv ist.

| | | |
|---|---|---|
| Request Data | - | **20** NetFnlLUN: Firmware |
| | - | **04** CMD : Command Group Firmware |
| | 1 | Selector:<br>0 = Auto (Firmware Image mit der neuesten Firmware-Version.)<br>1 = low firmware image<br>2 = high firmware image<br>3 = Auto oldest version (Firmware Image mit der ältesten Firmware-Version.)<br>4 = MRP (Firmware Image mit der zuletzt aktualisierten Firmware)<br>5 = LRP (Firmware Image mit der am längsten nicht mehr aktualisierten Firmware) |
| Response Data | - | **24** |
| | - | **04** |
| | 1 | Completion Code |

### 20 05 - Get Firmware Selector

Dieses Kommando liefert die Einstellungen des aktuellen Firmware Selectors .

| | | |
|---|---|---|
| Request Data | - | **20** NetFnlLUN: Firmware |
| | - | **05** CMD : Command Group Firmware |
| Response Data | - | **24** |
| | - | **05** |
| | 1 | Completion Code |
| | 2 | Next Boot Selector:<br>0 = Auto (Firmware Image mit der neuesten Firmware-Version)<br>1 = low EEPROM<br>2 = high EEPROM<br>3 = Auto oldest version (EEPROM mit der ältesten Firmware-Version)<br>4 = MRP (Firmware Image mit der zuletzt aktualisierten Firmware)<br>5 = LRP (Firmware Image mit der am längsten nicht mehr aktualisierten Firmware) |
| | 3 | Running Selector; zeigt an, welcher EEPROM aktiv ist:<br>1 = low EEPROM<br>2 = high EEPROM |

### C0 19 - Get Remote Storage Connection or Status

Dieses Kommando informiert je nach Parametrisierung,

– ob Remote Storage-Verbindungen bestehen,
– über Status und Typ der Remote Storage-Verbindung(en).

Wenn *Request Data 1* auf "1" gesetzt ist, informiert das Kommando, ob Speichermedien als Remote Storage verbunden sind.

| | | |
|---|---|---|
| Request Data | - | **C0** NetFnlLUN: OEM |
| | - | **19** CMD : Command Group Firmware |
| | 1 | 01 |
| | 2 | 00 |
| | 3 | 00 |
| Response Data | - | **C4** |
| | - | **19** |
| | 1 | Completion Code |
| | 2 | **01** |
| | 3 | **00: No**<br>**01: Ja, verbunden** |
| | 4 | **00** |
| | 5 | **00** |

Wenn *Request Data 1* auf "2" gesetzt ist, informiert das Kommando über Status und Typ der Remote Storage-Verbindung(en).

| | | |
|---|---|---|
| Request Data | - | **C0** NetFnlLUN: OEM |
| | - | **19** CMD : Command Group Firmware |
| | 1 | 02 |
| | 2 | 00 |
| | 3 | 00 = Connection 0<br>01 = Connection 2 |
| Response Data | - | **C4** |
| | - | **19** |
| | 1 | Completion Code |
| | 2 | **02** |
| | 3 | **00** |
| | 4 | **00** |
| | 5 | **00 = Invalid / unknown**<br><br>**01 = idle**<br><br>**02 = Connection Attempt pending**<br><br>**03 = Connected**<br><br>**04 = Connection Attempts retries exhausted / failed**<br><br>**05** = **Connection lost**<br><br>**06** = **Disconnect pending** |
| | 6 | 00 **= Invalid / unknown**<br>**01 = Storage Server / IPMI**<br><br>**02 = Applet**<br><br>**03 = None / Not connected** |

### C0 1A - Set Video Display On/Off

Dieses Kommando ermöglicht das Ein- und Ausschalten der lokalen Konsole.

| | | |
|---|---|---|
| Request Data | - | **C0** NetFnlLUN: OEM |
| | - | **1A** Cmd : Command Group Fan Test |
| | 1 | 00 = Set Video Display On<br>01 = Set Video Display Off |
| Response Data | - | **C4** |
| | - | **1A** |
| | 1 | Completion Code |

## 12.1.2.6 BIOS-spezifische Kommandos

### F1 09 - Get BIOS POST State

Dieses Kommando informiert, ob sich das BIOS in der POST-Phase befindet.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F1** Cmd : Command Group BIOS |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 4 | **09** Command Specifier |
| Response Data | - | **BC** |
| | - | **F1** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 5 | [7:1] - reserved<br>[0] - BIOS POST State : 0 = BIOS is not in POST<br>1 = BIOS is in POST |

### F1 15 - Get CPU Info

Dieses Kommando liefert CPU-interne Informationen. Der iRMC S4 empfängt diese Information während der POST-Phase das BIOS.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F1** Cmd : Command Group BIOS |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 4 | **15** Command Specifier |
| | 5 | Socket Number (0-based) of the CPU |
| Response Data | - | **BC** |
| | - | **F1** |
| | 1 | **Completion Code:**<br>01 = Unpopulated CPU Socket |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 5:6 | CPU ID, LS Byte first |
| | 7 | Platform ID |
| | 8 | Brand ID |
| | 9:10 | Maximal Core Speed of the CPU [MHz], LS Byte first |
| | 11:12 | Intel Qickpath Interconnect in Mega Transactions per second, LS Byte first |
| | 13 | T-Control Offset |
| | 14 | T-Diode Offset |
| | 15 | CPU data Spare |
| | 16:17 | Record ID CPU Info SDR, LS Byte first |
| | 18:19 | Record ID Fan Control SDR, LS Byte first |
| | 20:21 | CPU ID High Word, LS Byte first (0 if none) |

### 12.1.2.7 iRMC S4-spezifische Kommandos

#### F5 10 - Get System Status

Dieses Kommando liefert eine Vielzahl interner Informationen über den Server, wie z. B. Power- oder Fehlerstatus.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group Memory |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **10** Command Specifier |
| | 5:8 | **Timestamp** |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 5 | **System Status** (Details siehe unten.) |
| | 6 | **Signaling** (Details siehe unten.) |
| | 7 | **Notifications** (Details siehe unten.) |
| | 8 | **POST Code** |

Der Zeitstempel (Timestamp) wird nur für die Auswertung des *Notifications*-Byte benötigt.

**System Status**

Bit 7 - System ON

Bit 6 -

Bit 5 -

Bit 4 - SEL entries available

Bit 3 -

Bit 2 - Watchdog active

Bit 1 - Agent connected

Bit 0 - Post State

**Signaling**

Bit 7 - Localize LED

Bit 6 -

Bit 5 -

Bit 4 -

Bit 3 - CSS LED

Bit 2 - CSS LED

Bit 1 - Global Error LED

Bit 0 - Global Error LED

**Notifications**

Bit 7 - SEL Modified (New SEL Entry)

Bit 6 - SEL Modified (SEL Cleared)

Bit 5 - SDR Modified

Bit 4 - Nonvolatile IPMI Variable modified

Bit 3 - ConfigSpace Modified

Bit 2 -

Bit 1 -

Bit 0 - New Output on LocalView panel

### F5 12 - Get EEPROM Version Info

Dieses Kommando informiert über die aktuellen Versionen von Bootloader, Firmware und SDR in den EEPROMs.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group Memory |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **12** Command Specifier |
| | 5 | EEPROM# 00=EEPROM 1; 01=EEPROM 2 |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 5 | **Status** 00=Checksum Error Runtime FW, 01=OK |
| | 6 | **Major FW Revision** Binary coded |
| | 7 | **Minor FW Revision** BCD coded |
| | 8:10 | **Aux. FW Revision** Binary coded (major/minor/res.) |
| | 11 | **Major FW Revision** ASCII coded letter |
| | 12 | **Major SDRR Revision** BCD coded |
| | 13 | **Minor SDRR Revision** BCD coded |
| | 14 | **SDRR Revision Char.** ASCII coded letter |
| | 15 | **SDRR-ID** LSB binary coded |
| | 16 | **SDRR-ID** MSB binary coded |
| | 17 | **Major Booter Revision** Binary coded |
| | 18 | **Major Booter Revision** BCD coded |
| | 19:20 | *Aux. Booter Revision* Binary coded (major/minor) |

### F5 42 - Get HDD lightpath status (Component Status Signal Read)

Dieses Kommando gibt Informationen zum Status des Festplatten-Steckplatzes (HDD) zurück.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFn\|LUN: OEM/Group |
| | - | **F5** Cmd : Command Group iRMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 4 | **42** Command Specifier |
| | 5 | **Entity ID** (*Tabelle 37-12* in der IPMI 1.5 Spez.) der Komponente, dessen Statussignal gelesen werden soll. |
| | 6 | **Entity Instance** (0-basiert) der Komponente, dessen Statussignal gelesen werden soll. |
| | 7 | **Sensor Type** (*Tabelle 36-3* der IPMI-Spez.) des Sensors, der den Status der Komponente meldet, der das Statussignal zugeordnet wird. |
| | (8) | Option (optional)<br>Bit 7:2 - Reserved<br>Bit 1 :Completion Code 0x02 suppressed<br>Bit 0 - 1 : Return ID String of Component Status Sensor |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | **Completion Code:**<br>01= Statussignal nicht verfügbar<br>02 = Komponente nicht vorhanden |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 5 | **Signalstatus:**<br>00 = OK<br>01 = Identifizierung<br>02 = Prefailure-Warnung<br>03 = Fehler |
| | 6 | **CSS und physische LED verfügbar:**<br>Bit 6:0 - 0 = keine physische LED verfügbar<br>Bit 6:0 > 00 = Physische LED verfügbar; ein- oder mehrfarbig, Code<br>Bit 7 = 0: Keine CSS-Komponente<br>Bit 7 = 1: CSS-Komponente |
| | (7) | Länge des ID-Strings des Komponenten-Status-Sensors (nur vorhanden, wenn Bit 0 in Request Byte 8 festgelegt wurde) |

| | |
|---|---|
| (8 .. m) | Länge des ID-Strings des Komponenten-Status-Sensors in ASCII-Zeichen<br>(nur vorhanden, wenn Bit 0 in Request Byte 8 festgelegt wurde) |

### F5 43 - Get SEL entry long text

Dieses Kommando übersetzt einen vorliegenden System Event Log (SEL) in Klartext.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFn\|LUN: OEM/Group |
| | - | **F5** Cmd : Command Group iRMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 4 | **43** Command Specifier |
| | 5:6 | **Record ID** des SEL-Datensatzes, LS Byte first 0x0000: ersten Datensatz abrufen 0xFFFF: letzten Datensatz abrufen |
| | 7 | **Offset** als Antwort auf SEL-Text |
| | 8 | **MaxResponseDataSize** Größe von *Konvertierte SEL-Daten* (16:n) als Antwort |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code: |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 5:6 | Next Record ID |
| | 7:8 | **Actual Record ID** |
| | 9 | **Record type** |
| | 10:13 | **Timestamp** |
| | 14 | **Severity:** Bit 7: 0 = No CSS component<br>1 = CSS component<br>Bit 6-4: 000 = INFORMATIONAL<br>001 = MINOR<br>010 = MAJOR<br>011 = CRITICAL<br>1xx = Unknown'<br>Bit 3-0: reserved, read as 0000 |
| | 15 | **Länge der Daten** des gesamten Texts |
| | 16:n | **Konvertierte SEL-Daten** angefordertes Teil (n = 16 + MaxResponseDataSize - 1) |
| | n + 1 | **String Terminator** nachfolgendes '\0'-Zeichen |

### F5 45 - Get SEL entry text

Dieses Kommando übersetzt einen vorliegenden Fehlerspeicher (System Event Log, SEL) in ASCII-Text.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group iRMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 4 | **45** Command Specifier |
| | 5:6 | **Record ID** von SDR, LS Byte first |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte first |
| | 5:6 | **Next Record ID** |
| | 7:8 | **Actual Record ID** |
| | 9 | **Record type** |
| | 10:13 | **Timestamp** |
| | 14 | **Severity:** Bit 7: 0 = No CSS component<br>1 = CSS component<br>Bit 6-4: 000 = INFORMATIONAL<br>001 = MINOR<br>010 = MAJOR<br>011 = CRITICAL<br>1xx = Unknown'<br>Bit 3-0: reserved, read as 0000 |
| | 15 | **Data length** |
| | 16:35 | **Converted SEL data** |

### F5 B0 - Set Identify LED

Mithilfe dieses Kommandos können Sie die Identifizierungs-LED (blau) des Servers ein- und ausschalten. Darüber hinaus können Sie die GPIOs festlegen und lesen, die direkt mit der Identify LED verbunden sind.

Die Identify LED können Sie außerdem über den Identify Button am Servers ein- und ausschalten.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group BMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **B0** Command Specifier |
| | 5 | **Identify LED:**<br>0: Identify LED aus<br>1: Identify LED ein |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

### F5 B1 - Get Identify LED

Dieses Kommando informiert über den Status der Identify-LED (blau) des Servers.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group BMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **B1** Command Specifier |
| Response Data | - | **BC** |
| | - | F5 |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 5 | Status der Identify LED (nur Bit 0 ist relevant) |

### F5 B3 - Get Error LED

Dieses Kommando informiert über den Status der Global Error LED (rot) und der CSS LED (gelb) des Servers. Die Global Error LED zeigt die schwerwiegendsten Fehler-Status der Komponenten an. Die CSS LED zeigt an, ob Fehler vorliegen, die Sie als Kunde selber beheben können.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group BMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **B3** Command Specifier |
| Response Data | - | BC |
| | - | F5 |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 5 | **Fehlerstatus-LED:**<br>0 : CSS ausgeschaltet/GEL ausgeschaltet<br>1 : CSS ausgeschaltet/GEL eingeschaltet<br>2 : CSS ausgeschaltet/GEL blinkt<br>3 : CSS eingeschaltet/GEL ausgeschaltet<br>4 : CSS eingeschaltet/GEL eingeschaltet<br>5 : CSS eingeschaltet/GEL blinkt<br>6 : CSS blinkt/GEL ausgeschaltet<br>7 : CSS blinkt/GEL eingeschaltet<br>8 : CSS blinkt/GEL blinkt |

### F5 DF - Reset Nonvolatile Cfg Variables to Default

Dieses Kommando setzt alle nicht-flüchtigen IPMI Settings auf Default-Werte.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group BMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **DF** Command Specifier |
| | 5:8 | 43 4C 52 AA = 'CLR'0xaa: Sicherheitscode |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

### F5 E0 - Reset ConfigSpace Variables to Default

Dieses Kommando setzt alle Variablen des Configuration Space auf Default-Werte.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group BMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **E0** Command Specifier |
| | 5:8 | 43 4C 52 AA = 'CLR'0xaa: Sicherheitscode |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

### F5 F8 - Delete User ID

Das System unterstützt bis zu 16 Benutzer. Mit diesem Kommando können Sie einzelne iRMC S4-Benutzerkennungen löschen.

**ACHTUNG!**

Wenn Sie alle iRMC S4-Benutzerkennungen löschen, kann das System nicht mehr verwaltet werden.

| | | |
|---|---|---|
| Request Data | - | **B8** NetFnlLUN: OEM/Group |
| | - | **F5** Cmd : Command Group BMC |
| | 1:3 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |
| | 4 | **F8** Command Specifier |
| | 5:8 | Benutzerkennung (1-16) |
| Response Data | - | **BC** |
| | - | **F5** |
| | 1 | Completion Code |
| | 2:4 | **80 28 00** IANA-Enterprise-Number FTS, LS Byte First |

# 12.2 iRMC S4 mit SCCI und per Skript-Konfiguration konfigurieren

Der vorliegende Abschnitt informiert über folgende Themen:

– Verwenden einer SCCI-konformen (**S**erverView **C**ommon **C**ommand **I**nterface) Schnittstelle zum Konfigurieren des iRMC S4.

– Skript-Konfiguration des iRMC S4

## 12.2.1 iRMC S4-Konfigurationsdaten

Beachten Sie, dass die nachfolgend beschriebene Schnittstelle hauptsächlich für eine Remote-Konfiguration gilt und **keine** SCCI-Implementierung ist. Es werden nur die SCCI-Kommando- und -Konfigurationsdefinitionen und das SCCI-Dateiformat verwendet.

### 12.2.1.1 Überblick

Der iRMC S4 speichert interne Konfigurationsdaten in separaten Abschnitten des NVRAM (Non-Volatile RAM):

– FTS-spezifische ConfigSpace-Daten, die von der Firmware über eine interne Beschreibung oder Zuordnungstabelle aufgerufen werden.

– Ursprüngliche, herstellerspezifische OMD NVCFG-Daten, auf die von den Offset-Definitionen zugegriffen wird.

Einige Konfigurationsdaten der ursprünglichen OMD NVCFG-Daten werden intern von der Firmware zugeordnet, damit mithilfe von ConfigSpace-Zugriffsmethoden darauf zugegriffen werden kann. Der Zugriff auf DNS-Server und die DNS-Konfiguration des iRMC S4 ist über IPMI OEM LAN-Konfigurationsparameter und über ConfigSpace möglich. Mit beiden Methoden wird auf die gleichen Datenstrukturen der unteren Stufe im Original-NVCFG-Abschnitt zugegriffen.

Nicht-iRMC S4-spezifische ServerView-Softwarekomponenten (z.B. die ServerView Agents oder der Server Configuration Manager) ordnen in manchen Fällen auch Standard-IPMI-verwandte Kommandos und Konfigurationselemente zu, z.B. Standard-IPMI-Benutzerkonfiguration oder IPv4-Netzwerkkonfiguration. Dadurch wird eine Abstraktionsebene zwischen der IPMI BMC-Ebene und höheren Softwareebenen implementiert.

Das SCCI ist eine generische Anwendungsprogrammierschnittstelle (API), die von Fujitsu für verschiedene Server Management Controller-Hardware sowie Server Management-Software (z. B. ServerView Agents) definiert wird. Sie kann mühelos erweitert werden, um neue Kommandos oder neue Konfigurationselemente zu umfassen. Eine Architekturübersicht des SCCI finden Sie in der Online-Hilfe für die ServerView Agents.

Der iRMC S4 unterstützt eine Remote-Konfiguration und eingeschränkte Skripterstellung über die */config URL* im iRMC S4.

### Vorteile einer iRMC S4-Remote-Konfiguration über einen Web-basierten Zugriff

Die Remote-Konfiguration von iRMC S4 über einen Web-basierten Zugriff bietet die folgenden Vorteile:

– Verwendet die HTTP POST-Operation zum Hochladen von Dateien in den iRMC S4. Es sind keine speziellen Tools erforderlich. Jedes allgemeine Tool oder jede Scriptumgebung, die authentifizierte HTTP POST-Operationen unterstützen, können verwendet werden. Beispiel-Skripte befinden sich auf der ServerView Suite DVD 2

– Verwendet integrierte Authentifizierungs- und Autorisierungsmethoden des iRMC S4-Webservers.

– Unterstützt die HTTP 1.1 Basic- und Digest-Authentifizierung basierend auf RFC 2617 mit lokalen iRMC S4-Benutzerkonten.

– Bietet optional integrierte leistungsstarke Verschlüsselung mit standardmäßig HTTPS-basiertem Zugriff.

– Kann mit globalen Benutzerkonten (verwaltet durch einen LDAP-Verzeichnisdienst) und HTTP 1.1 Basic-Authentifizierung verwendet werden.

  Wenn die HTTP 1.1 Basic-Authentifizierung verwendet wird, wird aus Verschlüsselungs- und Vertraulichkeitsgründen empfohlen, das HTTPS-Protokoll zu verwenden, um die Benutzername-Kennwort-Kombination zu schützen.

– Verwendet ein auf XML basierendes Konfigurationsdateiformat. Sie haben die Möglichkeit, die Datei manuell zu bearbeiten oder sie aus einer Referenzinstallation oder dem Server Configuration Manager zu exportieren.

Die Konfigurationsdatei kann mit anderen SCCI-basierten Installationsmethoden (z. B. Server Configuration Manager) erneut verwendet werden.

– Es ist eine mühelose Erweiterung auf neue Konfigurationselemente und neu unterstützte SCCI-Kommandos möglich.

#### 12.2.1.2 SCCI-Dateiformat

Das Format der verwendeten XML-Konfigurationsdatei (*.pre*) stammt aus der Setup-Konfigurationshilfedatei, die zusammen mit den ServerView Agents unter Windows installiert wird. Eine Kopie dieser Beschreibung mit iRMC S4-spezifischen Hinweisen wird unten aufgeführt.

Die Konfigurationsdatei basiert auf einer XML-Syntax:

– Jede Konfigurationseinstellung besteht aus einem einfachen XML-Fragment, das mit einem „<CMD>“-Tag beginnt.

– Die vollständige Sequenz der Konfigurationseinstellungen befindet sich zwischen dem Tag-Paar „<CMDSEQ>“ und „</CMDSEQ>“.

Im Folgenden finden Sie ein Beispiel für eine typische Kommandosequenz mit zwei Konfigurationseinstellungen:

```
<CMDSEQ>
<CMD Context="SCCI" OC="ConfigSpace" OE="3800" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">04</DATA>
<CMD Context="SCCI" OC="ConfigSpace" OE="3801" OI="0"
Type="SET">
<DATA Type="xsd::hexBinary" Len="1">00</DATA> </CMD>
</CMDSEQ>
```

Der Parameter *Context* wird intern zur Auswahl des Anbieters der Operation verwendet. Derzeit ist `SCCI` der einzige unterstützte Anbieter.

### Parameter von SCCI-Anbieter-spezifischen Kommandos

Die folgenden SCCI-Anbieter-spezifischen Kommandos stehen zur Verfügung:

Operationscode (`OC`)
: Hexadezimalwert oder String, der das Kommando bzw. den Operationscode festlegt.

  > **i** Der iRMC S4 unterstützt nur einen eingeschränkten Satz an SCCI-Kommandos. Eine Liste der unterstützten Kommandos finden Sie unter table "Vom iRMC S4 unterstützte SCCI-Kommandos" on page 489

Operationscode-Erweiterung (`OE`)
: Hexadezimalwert für erweiterten Operationscode. Standard: `OE=0`

  Bei ConfigSpace-Lese-/Schreibvorgängen definiert dieser Wert die ConfigSpace-ID.

Objektindex (`OI`)
: Hexadezimalwert zur Auswahl einer Objektinstanz. Standard: OI=0"

Operationscode-Typ (`Type`)
: Bei Konfigurationseinstellungen werden die Werte `GET` (Lesevorgang) und `SET` (Schreibvorgang) unterstützt. Standard: Type=GET

  > **i** Bei `SET`-Operationen sind Daten erforderlich. Verwenden Sie zum Angeben des entsprechenden Datentyps den unten beschriebenen Parameter *Data (DATA)*.

Gehäuse-ID (`CA`)
: Ermöglicht es Ihnen, ein Erweiterungsgehäuse auszuwählen und die Gehäuse-ID zu verwenden.

  > **i** Verwenden Sie diesen Parameter **nicht**, um das Systemgehäuse anzufordern!

Daten (`DATA`)
: Bei angegebenem `SET`-Parameter (Schreibvorgang): Datentyp (`Type`-Parameter) und, in einigen Fällen, Länge der Daten (`LEN`-Parameter) sind erforderlich.

  Derzeit werden die folgenden Datentypen unterstützt:

  – `xsd::integer`

    Ganzzahl

*Beispiel*

```
<DATA Type="xsd::integer">1234</DATA>
```

– `xsd::hexBinary`

Byte-Stream. Jedes Byte wird mit zwei ASCII-Zeichen codiert. Verwenden Sie den `Len`-Parameter wie im unten stehenden Beispiel gezeigt, um die Länge des Streams festzulegen (d. h. die Anzahl der Bytes).

Der Datentyp `xsd::hexBinary` kann ohne Einschränkung verwendet werden. Die Anzahl genutzter Bytes wird anhand des Parameters *Len* bestimmt.

*Beispiel*

Ein Stream aus vier Bytes `0x00 0x01 0x02 0x04` wird als folgender ASCII-Stream codiert:

```
<DATA Type="xsd::hexBinary" Len="4">0001020304</DATA>
```

– `xsd::string`

Normalerweise zur Übertragung der Strings verwendet. Darüber hinaus kann der Typ `string` für IPv4-Adressen und MD5-basierte Benutzerkennwörter verwendet werden. In diesem Fall werden die String-Daten intern in das akzeptierte Zielformat konvertiert.

*Verschlüsselte Daten übertragen*

Eine Fujitsu-eigene Datenverschlüsselung wird bei einigen vertraulichen Daten unterstützt, z.B. Benutzer- oder Dienstzugriffskennwörter (LDAP/SMTP) oder für den AVR-Lizenzschlüssel des iRMC S4. Mit dem Programm *iRMC_PWD.exe* können Sie Kennwortdaten verschlüsseln (siehe section "Verschlüsselte Kennwörter mit dem Programm iRMC_PWD.exe generieren" on page 493).

`Encrypted="1"` muss im Tag `<DATA>` festgelegt werden, um anzugeben, dass die zu schreibenden Daten verschlüsselt sind.

*Beispiele*

String „Hello World“ übertragen:

```
<DATA Type="xsd::string">Hello World</DATA>
```

Kennwort als reinen (lesbaren) Text übertragen:

```
<DATA Type="xsd::string">Eigenes lesbares
Kennwort</DATA>
```

Verschlüsseltes Kennwort übertragen:

```
<DATA Type="xsd::string"
Encrypted="1">TpVlTJwCyHEIsC8tk24ci83JuR9l</DATA>
```

Transferring the IPv4 address "192.23.2.4"

```
<DATA Type="xsd::string">192.23.2.4</DATA>
```

**ACHTUNG!**

Der Datentyp `xsd::string` ist auf lesbare Strings, IP-Adressen und MD5-basierte Benutzerkennwörter beschränkt.

Bei allen anderen Daten muss der Datentyp `xsd::hexbinary` verwendet werden.

**Geben Sie die Zeichen ä, ö, ü usw. in Strings nicht direkt an, es sei denn, sie werden von der jeweiligen Anwendung benötigt.**

Weder die SCCI- noch die ConfigSpace-Schnittstelle speichern Informationen zur Zeichencodierung. Daher werden alle Nicht-US-ASCII-Zeichen intern von der verwendenden Anwendung interpretiert und sollten vermieden werden.

Wenn Sie Sonderzeichen angeben müssen, stellen Sie sicher, dass Sie Ihre Datei im UTF-8-Format und mit dem korrekten BOM bearbeiten und speichern.

Kommandostatus (`Status`)

Nach der Übertragung der Konfigurationseinstellungen enthält der `Status` das Ergebnis der Operation. Wenn die Operation erfolgreich abgeschlossen wurde, wird der Wert `0` zurückgegeben.

Eine Spezifikation aller öffentlichen Konfigurationseinstellungen (ConfigSpace) finden Sie in der Datei *SCCI_CS.pdf*, die mit dem PRIMERGY Scripting Toolkit verteilt wird.

#### 12.2.1.3 Einschränkungen

Alle in der *.pre*-Datei angegebenen Kommandos werden normalerweise in der angegebenen Reihenfolge ausgeführt. Die folgenden Ausnahmen weichen von dieser Regel ab:

– Um eine Unterbrechung der Netzwerkverbindung zu verhindern, werden Kommandos für die IPv4- und VLAN-Netzwerkkonfiguration am Ende einer Kommandosequenz ausgeführt.

– Die IPv6-Konfiguration ist derzeit auf die Konfiguration von nicht-flüchtigen IPv6-Konfigurationsparametern beschränkt.

  Als Workaround könnten Sie folgendermaßen vorgehen:

  1. Ordnen Sie das Script folgendermaßen an:
     a) Zu Beginn des Scripts: Deaktivieren Sie IPv6.
     b) Konfigurieren Sie IPv6-Parameter.
     c) Am Ende des Scripts: Aktivieren Sie IPv6.
  2. Übertragen Sie das Script von einer IPv4-Adresse.

– Das SSL-Zertifikat und der entsprechende passende private Schlüssel werden am Ende einer Kommandosequenz ausgeführt. Beide Komponenten müssen in der gleichen *.pre*-Datei angegeben sein und werden auf Übereinstimmung überprüft.

– Wenn eine Energieverwaltungsoperation für den verwalteten Server oder ein Neustart des iRMC S4 erfordert oder erwünscht ist:

  Es wird empfohlen (es ist jedoch nicht erforderlich), dass Sie diese Kommandos in separaten Kommandodateien ausführen. Unterteilen Sie dazu beispielsweise die Konfigurations- und Energieverwaltungsvorgänge in separate Aufgaben.

– Optional müssen Zeitverzögerungen zwischen der Ausführung der aufeinander folgenden Kommandos außerhalb des Scripts implementiert werden.

  Dies können Sie folgendermaßen umsetzen:

  1. Unterteilen Sie das Skript in angemessene separate Skripte.
  2. Verwenden Sie den Funktionsbereich des Clients, um Zeitverzögerungen zwischen dem Versenden der einzelnen Dateien einzufügen.

#### 12.2.1.4 Konfigurationsdaten des iRMC S4 exportieren/importieren

Über die Seite *Save iRMC S4 Firmware Settings* im iRMC S4-Web-Interface können Sie die aktuellen iRMC S4-Konfigurationsdaten in einer Konfigurationsdatei (*.pre*) speichern (exportieren). Zudem können Sie die iRMC S4-Konfigurationsdaten aus einer bestehenden Konfigurationsdatei (*.pre*) importieren, d.h. die Konfigurationsdaten in den iRMC S4 laden. (Details siehe section "iRMC S4 Firmware Einstellungen abspeichern - Firmware-Einstellungen abspeichern" on page 198.)

Zum Importieren einer iRMC S4-Konfiguration können Sie alternativ die entsprechende SCCI-Kommando-Datei an die */config URI* des iRMC S4 mittels einer HTTP POST-Operation senden.

## 12.2.2 Skript-Konfiguration des iRMC S4

Der vorliegende Abschnitt informiert über folgende Themen:

– Vom iRMC S4 unterstützte SCCI-Kommandos

– Verwenden von verschiedenen Skript-Sprachen für die Skript-Konfiguration des iRMC S4

– Generieren von verschlüsselten Kennwörtern mit dem Programm *iRMC_PWD.exe*

### 12.2.2.1 Liste der vom iRMC S4 unterstützten SCCI-Kommandos

Die vom iRMC S4 unterstützten SCCI-Kommandos finden Sie in table 25:

| SCCI-Operationscode | SCCI-Kommando-String | Beschreibung |
|---|---|---|
| 0xE002 | ConfigSpace | ConfigSpace-Schreibvorgang |
| 0x0111 | PowerOnCabinet | Server einschalten |
| 0x0112 | PowerOffCabinet | Server ausschalten |
| 0x0113 | PowerOffOnCabinet | Server aus-/einschalten |
| 0x0204 | ResetServer | Hard-Reset des Servers |
| 0x020C | RaiseNMI | NMI (Non Maskable Interrupt) auslösen |
| 0x0205 | RequestShutdownAndOff | System herunterfahren, Agent muss ausgeführt werden |
| 0x0206 | RequestShutdownAndReset | Systemneustart, Agent muss ausgeführt werden |
| 0x0209 | ShutdownRequestCancelled | Shutdown-Anforderung abbrechen |
| 0x0203 | ResetFirmware | BMC-Reset durchführen |
| 0x0250 | ConnectRemoteFdImage | Ein Disketten-Image auf einem remoten Image-Mount (NFS oder CIFS-Freigabe) verbinden oder trennen |
| 0x0251 | ConnectRemoteCdImage | Ein CD/DVD-ISO-Image auf einem remoten Image-Mount (NFS oder CIFS-Freigabe) verbinden oder trennen |
| 0x0252 | ConnectRemoteHdImage | Ein Festplatten-Image auf einem remoten Image-Mount (NFS oder CIFS-Freigabe) verbinden oder trennen |

Table 25: Vom iRMC S4 unterstützte SCCI-Kommandos

#### 12.2.2.2 Skripte mit cURL

Das Open-Source-Kommandozeilen-Tool cURL ermöglicht es Ihnen, Daten mit einer URL-Syntax zu übertragen. Sie können die aktuelle Version des Quellcodes sowie vorab kompilierte Versionen für verschiedene Betriebssysteme unter *http://curl.haxx.se/* herunterladen.

Im Folgenden finden Sie einige Beispiele, wie Sie mit cURL eine Konfigurationsdatei an den iRMC S4 senden können.

Details zu den cURL-Kommandozeilenoptionen finden Sie in der cURL-Dokumentation.

– HTTP-Zugriff mit Basic-Authentifizierung (Standard) und das standardmäßige iRMC S4-Admin-Konto:

```
curl --basic -u admin:admin --data @Config.pre
http://<IP-Adresse des iRMC S4>/config
```

– HTTP-Zugriff mit Digest-Authentifizierung und das standardmäßige iRMC-Admin-Konto:

```
curl --digest -u admin:admin --data @Config.pre
http://<IP-Adresse des iRMC S4>/config
```

– HTTPS-Zugriff ohne Zertifikatsprüfung (-k) und Digest-Authentifizierung und das standardmäßige iRMC-Admin-Konto:

```
curl --digest -k -u admin:admin --data @Config.pre
https://<IP-Adresse des iRMC S4>/config
```

– HTTPS-Zugriff mit einem LDAP-Benutzerkonto.

  Beachten Sie, dass Sie für LDAP-Benutzer die Basic-Authentifizierung angeben müssen.

```
curl --basic -k -u LDAPuser:LDAPpassword --data @Config.pre
https://<IP-Adresse des iRMC S4>/config
```

#### 12.2.2.3 Skripte mit Visual Basic (VB) Script

Mit dem folgenden VB-Script wird eine Konfigurationsdatei an den iRMC S4 gesendet:

```
IP_ADDRESS = "<iRMC S4 IP-Adresse>"
USER_NAME  = "admin"
PASSWORD   = "admin"

FILE_NAME  = ".\\ConfigFile.pre"

Const ForReading = 1
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objFile = objFSO.OpenTextFile(FILE_NAME, ForReading)

' ---------------------------------------------------------------------
On Error Resume Next

Set xmlHttp = CreateObject("Microsoft.XMLHTTP")
xmlHttp.Open "POST", "http://" & IP_ADDRESS & "/config", False,
USER_NAME, PASSWORD
xmlhttp.setRequestHeader "Content-Type", "application/x-www-
form-urlencoded"
xmlHttp.Send objFile.ReadAll

Wscript.Echo xmlhttp.responsexml.xml
```

#### 12.2.2.4 Skripte mit Python

```
#!/usr/bin/python3
import sys
import httplib2
from urllib.parse import urlencode

# ============================================================
# iRMC

USER = 'admin'
PWD  = 'admin'
IP_ADDR = '192.168.1.100'
# ============================================================

h = httplib2.Http()

# Basic/Digest authentication
h.add_credentials(USER, PWD)

def doit(data,ausgabe=sys.stdout):
  try:
    resp, content = h.request("http://%s/config" % IP_ADDR,
    "POST", data)
    if resp['status'] == '200'
      data = content.decode('utf-8')
      print(data,file=ausgabe)
      else:
      print('STATUS:',resp['status'],file=ausgabe)
      print(str(resp),file=ausgabe)
  except Exception as err:
    print('ERROR:',str(err),file=ausgabe)
  print()


# Beispiel 1 - Konfigurationsdatei an den iRMC S4 senden
try:
  data = open('ConfigFile.pre').read()
  doit(data)
except Exception as err:
  print('ERROR:',str(err),file=ausgabe)


# Beispiel 2 - ConfigSpace-Werte festlegen
# 0x200 (ConfCabinetLocation) und
# 0x204 (ConfSystemContact) direkt aus Script
#
LocationContact = '''<?xml version="1.0" encoding="UTF-8"
standalone="yes" ?>
```

```
<CMDSEQ>
  <!-- ConfCabinetLocation -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="200" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
  <!-- ConfSystemContact -->
  <CMD Context="SCCI" OC="ConfigSpace" OE="204" OI="0" >
    <DATA Type="xsd::string">%s</DATA>
  </CMD>
</CMDSEQ>
'''

doit(LocationContact % ("Ostsee","Kiel"))
```

#### 12.2.2.5 Verschlüsselte Kennwörter mit dem Programm iRMC_PWD.exe generieren

Das Hilfsprogramm von Fujitsu Technology Solutions zur iRMC-Kennwortverschlüsselung und -prüfung *iRMC_PWD.exe* ist ein Win32-Programm, mit dem Sie verschlüsselte Kennwörter für SCCI-Scripte generieren können. Mit *iRMC_PWD.exe* können Sie ein einzelnes Kennwort verschlüsseln und eine SCCI-Batch-Datei für die Script-Konfiguration generieren.

**iRMC_PWD Standard-Kommandozeilenoptionen**

[-h] [-?]
: Diese Hilfe.

[-v]
: Überprüfen eines verschlüsselten Kennwort-Strings.

[-o] <oid>
: Die Objekt-ID für die zu verschlüsselnden Daten.

[-u] <username>
: Benutzername für die angegebene Objekt-ID (optional).

[-p] <password>
: Kennwort für die angegebene Objekt-ID / / zu prüfender verschlüsselter Kennwort-String.

[-x] <opCodeExt>
: Opcode-Erweiterung für die zu verschlüsselnden ConfigSpace-Daten.

[-p] <password>
Kennwort für die angegebene Objekt-ID.
Standard: 1452 (ConfBMCAcctUserPassword)

Unterstützte Werte:

1452 - ConfBMCAcctUserPassword

1273 - ConfAlarmEmailSMTPAuthPassword

197A - ConfLdapiRMCgroupsUserPasswd

502 - ConfBmcRadiusSharedSecret

1A52 - ConfBmcRemoteFdImageUserPassword

1A62 - ConfBmcRemoteCdImageUserPassword

1A72 - ConfBmcRemoteHdImageUserPassword

1980 - ConfBMCLicenseKey

### iRMC_PWD Kommandozeilenausgabe-Optionen

[-b]
Erstellt die Ergebnisdatei als WinSCU BATCH-Datei.

[-f] <Ergebnisdatei>
Festlegen des Ergebnisdateinamens.
Standard: *iRMC_pwd.txt*
Standard im Batch-Modus: *iRMC_pwd.pre*

*Beispiel*

Sie möchten eine *.pre*-Datei erstellen, mit der der Benutzername auf `admin` und das Kennwort auf `SecretPassword` für den (bestehenden) Benutzer mit der oid `2` festgelegt/geändert wird.

Geben Sie dazu das folgende Kommando ein:

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b
```

*iRMC_PWD* erstellt die *.pre*-Datei mit den in figure 261 on page 495 gezeigten Inhalten.

```
iRMC_PWD -o 2 -u admin -p SecretPassword -b


<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CMDSEQ>
<!-- "ConfBMCAcctUserName" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1451" OI="2" Type="SET">
  <DATA Type="xsd::string">admin</DATA>
  <STATUS>0</STATUS>
</CMD>
<!-- "ConfBMCAcctUserPassword" -->
<CMD Context="SCCI" OC="ConfigSpace" OE="1452" OI="2" Type="SET">
  <DATA Type="xsd::string"
Encrypted="1">N2BZd3oLHAgc11pnHCAV9P/ItwRue4qBB3IU7Xsh</DATA>
  <STATUS>0</STATUS>
</CMD>
</CMDSEQ>
```

Figure 261: Inhalte der generierten .pre-Datei

# 12.3 iRMC S4-System-Report

System Report ist eine der Funktionen von PRIME COLLECT. In der Regel werden die Informationen von den ServerView Agents erfasst, die unter dem Hostbetriebssystem ausgeführt werden, und umfassen verschiedene Arten an Hardware- und Softwareinformationen. Die erfassten Informationen enthalten unter anderem iRMC S4-Informationen (Sensor, IDPROM/FRU, Ereignisspeicher) sowie Angaben zu der auf dem Host installierten Software und den Treibern, laufenden Prozessen usw.

Auch wenn keine ServerView Agents ausgeführt werden, kann eine Teilmenge dieser Informationen, hauptsächlich bestehend aus Service-Vorfällen, direkt "Out-of-Band" vom iRMC S4 zur Verfügung gestellt werden.

Dieser Abschnitt beschreibt:

– Download per Skript und automatische Bewertung des iRMC S4-Reports

– Vom iRMC S4 bereitgestellte System-Report-Elemente.

## 12.3.1 Download per Skript und automatische Bewertung des iRMC S4-Reports

#### 12.3.1.1 Skripte mit cURL

Curl ist ein Open-Source-Befehlszeilen-Tool für die Übertragung von Daten, die mit URL-Syntax angegeben wurden. Sie können die aktuelle Version des Quellcodes sowie vorab kompilierte Versionen für verschiedene Betriebssysteme unter *http://curl.haxx.se/* herunterladen. Im Folgenden finden Sie einige Beispiele dazu, wie Sie die System Report-Datei mit cURL vom iRMC abrufen können. Details zu cURL-Befehlszeilenoptionen finden Sie in der cURL-Dokumentation. Standardmäßig sendet cURL die abgerufenen Daten an die Standardausgabe; Sie können sie dann weitergeben oder zur weiteren Verarbeitung umleiten oder die mit "–o outputfilename" abgerufenen Daten speichern.

– HTTP-Zugriff mit Digest-Authentifizierung, das standardmäßige iRMC-Admin-Konto und Speicherung (-o) in "report.xml":

```
curl --digest -o report.xml -u admin:admin
http://192.168.1.100/report.xml
```

– HTTPS-Zugriff ohne Zertifikatsprüfung (-k) und Digest-Authentifizierung und das standardmäßige iRMC-Admin-Konto:

```
curl --digest -k -u admin:admin
https://192.168.1.100/report.xml
```

– HTTPS-Zugriff mit einem LDAP-Benutzerkonto:

  Beachten Sie, dass Sie für LDAP-Benutzer die Basic-Authentifizierung angeben müssen, da die Authentifizierungsparameter zur Überprüfung an den LDAP-Server übergeben werden müssen:

```
curl --basic -k -u LDAPuser:LDAPpassword
https://192.168.1.100/report.xml
```

#### 12.3.1.2 Skripterstellung mit Visual Basic

Die Skripterstellung ist auch mit Visual Basic möglich. Mit dem folgenden VB-Skript wird "report.xml" vom iRMC abgerufen und in einer lokalen Datei gespeichert, die auch den Namen "report.xml" hat:

```
IP_ADRESSE = "192.168.1.100"
USER_NAME = "admin"
PASSWORD = "admin"
FILE_NAME = ".\\report.xml"
ADDONS = "/report.xml"
' ------------------------------------------------------------------
----------------------------------
On Error Resume Next
Function SaveBinaryData(FileName, ByteArray)
   Const adTypeBinary = 1
   Const adSaveCreateOverWrite = 2

   Dim BinaryStream
   Set BinaryStream = CreateObject("ADODB.Stream")

   BinaryStream.Type = adTypeBinary
   BinaryStream.Open
   BinaryStream.Write ByteArray
   BinaryStream.SaveToFile FileName, adSaveCreateOverWrite
   WScript.Echo "Antwort:" & BinaryStream.Read
End Function

Set xmlHttp = CreateObject("Msxml2.XMLHTTP")
xmlHttp.Open "GET", "http://" & IP_ADRESSE & ADDONS, False,
USER_NAME, PASSWORD
xmlHttp.Send

If InStr(xmlHttp.GetResponseHeader("Content-Type"), "xml") > 0
   Then
      SaveBinaryData FILE_NAME,xmlHttp.ResponseBody
```

```
   Else
   Wscript.Echo ADDONS &" not found on " &IP_ADRESSE
End If
```

## 12.3.2 Informationsabschnitte

### 12.3.2.1 Liste der unterstützten System Report-Abschnitte in der XML-Datei

| Abschnitt | Unterabschnitt | Anmerkungen/Einschränkungen |
|---|---|---|
| System | BIOS | Nur BIOS-Version-Zeichenfolge von ConfigSpace |
| | Processor | |
| | Memory | |
| | Fans | |
| | Temperatures | |
| | PowerSupplies | |
| | Voltages | |
| | IDPROMS | |
| | SensorDataRecords | |
| | PCIDevices | Nur PCI-Anbieter und Geräte-ID der Karten in den Steckplätzen, keine Onboard-Geräteinformationen |
| | SystemEventLog | |
| | InternalEventLog | |
| | BootStatus | |
| | ManagementControllers | Nur iRMC S4 |

Table 26: Liste der unterstützten System Report-Abschnitte in der XML-Datei

### 12.3.2.2 Abschnitt "Summary"

Die generierte XML-Datei enthält als ersten Abschnitt eine Zusammenfassung mit einigen Informationen hinsichtlich des Datums und der Uhrzeit der Erstellung, die aktuellen IP-Adressen des iRMC sowie eine Zusammenfassung der Anzahl an kritischen/schwerwiegenden und leichten (Warnung) Fehlern im Abschnitt "SystemEventLog". Zudem wird eine Liste der verfügbaren Abschnitte angezeigt.

Beispielausgabe siehe unten:

```
<?xml version="1.0" encoding="UTF-8"?>
<Root Schema="2" Version="97.30F" OS="iRMC S4">
   <Zusammenfassungen>
      <Created>
         <IsAdmin>true</IsAdmin>
         <Date>2014/02/05 17:27:15</Date>
         <BuildDuration>3</BuildDuration>
         <Company>FUJITSU</Company>
         <Computer>iRMCFDAF9F</Computer>
         <OS>iRMC S4 97.30F SDR: 3.32   ID 0342  TX140S2</OS>
         <Domain></Domain>
         <HostIPv4Address>10.172.103.13</HostIPv4Address>
         <HostIPv6Address>fe80::219:99ff:fefd:af9f</HostIPv6Addr
ess>
      <Created>
      <Errors Count="1">
         <Eventlog>
            <Message>59 important error(s) in event
log!</Message>
         </Eventlog>
      </Errors>
      <Warnings Count="1">
         <Eventlog>
            <Message>23 important warning(s) in event
log!</Message>
         </Eventlog>
      </Warnings>
      <Content>
         <Item Name="System/Bios"></Item>
         <Item Name="System/Processor"></Item>
         <Item Name="System/Memory"></Item>
         <Item Name="System/Fans"></Item>
         <Item Name="System/Temperatures"></Item>
         <Item Name="System/PowerSupplies"></Item>
         <Item Name="System/Voltages"></Item>
         <Item Name="System/IDPROMS"></Item>
         <Item Name="System/SensorDataRecords"></Item>
         <Item Name="System/PCIDevices"></Item>
         <Item Name="System/SystemEventlog"></Item>
         <Item Name="System/InternalEventlog"></Item>
         <Item Name="System/BootStatus"></Item>
         <Item Name="System/ManagementControllers"></Item>
      </Content>
    <Zusammenfassungen>
   <System>
```

#### 12.3.2.3 BIOS

Da der iRMC keinen Zugriff auf die SMBIOS-Strukturen des Servers hat, wird nur eine sehr begrenzte Teilmenge der Informationen bereitgestellt. Beispielausgabe siehe unten.

```
<Bios Schema="1">
   <SMBIOS Version="Unknown">
      <Type0 Name="BIOS Information" Type="0">
         <BiosVersion>V4.6.5.4 R1.0.0 for D3239-
A1x</BiosVersion>
      </Type0>
   </SMBIOS>
</Bios>
```

#### 12.3.2.4 Processor

Die generierten Informationen basieren auf den OEM IPMI-Befehlen F113 und F115 und sind mit der cDiagReport.h-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<Processor Schema="1">
   <CPU Boot="true">
      <SocketDesignation>CPU</SocketDesignation>
      <Manufacturer>Intel</Manufacturer>
      <Model>
         <Version>Intel(R) Xeon(R) CPU E3-1270 v3 @
3.50GHz</Version>
         <BrandName>Intel(R) Xeon(R) CPU E3-1270 v3 @
3.50GHz</BrandName>
      </Model>
      <Speed>3500</Speed>
      <Status Description="ok">1</Status>
      <CoreNumber>4</CoreNumber>
      <LogicalCpuNumber>8</LogicalCpuNumber>
      <Level1CacheSize Unit="KByte">256</Level1CacheSize>
      <Level2CacheSize Unit="KByte">1024</Level2CacheSize>
      <Level3CacheSize Unit="KByte">8192</Level3CacheSize>
   </CPU>
</Processor>
```

#### 12.3.2.5 Memory

Die generierten Informationen werden durch Entschlüsselung der Speicher-SPD-Daten sowie durch Bewerten des Speicherstatus und der Konfigurationssensoren abgerufen und sind mit der CDiagReport.h-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<Memory Schema="2">
   <Modules Count="4">
      <Module Name="DIMM-2A" CSS="true">
         <Status Description="empty">0</Status>
      </Module>
      <Module Name="DIMM-1A" CSS="true">
         <Status Description="ok">1</Status>
         <Approved>false</Approved>
         <Size Unit="GByte">2</Size>
         <Type>DDR3</Type>
         <BusFrequency Unit="MHz">1600</BusFrequency>
         <SPD Size="256" Revision="1.2" Checksum="true">
            <Checksum>
               <Data>33879</Data>
               <Calculated>33879</Calculated>
            </Checksum>
            <ModuleManufacturer>SK Hynix</ModuleManufacturer>
            <ModuleManufacturingDate>2013,4</ModuleManufacturing
             Date>
            <ModulePartNumber>HMT325U7EFR8A-PB
            </ModulePartNumber>
            <ModuleRevisionCode>12372</ModuleRevisionCode>
            <ModuleSerialNumber
AsString="4C633E39">1281572409</ModuleSerialNumber>
            <ModuleType>UDIMM</ModuleType>
            <DeviceType>DDR3_SDRAM</DeviceType>
            <DeviceTechnology>256Mx8/15x10x3</DeviceTechnology>
            <BufferedRegistered>None</BufferedRegistered>
            <BusFrequency Unit="MHz">DDR1600</BusFrequency>
            <VoltageInterface>1.35V/1.5V</VoltageInterface>
            <BurstLengths>8;(4);</BurstLengths>
            <CASLatencies>6;7;8;9;10;11;</CASLatencies>
            <DataWith>72</DataWith>
         </SPD>
         <ConfigStatus Description="Normal">0</ConfigStatus>
      </Module>
```

#### 12.3.2.6 Fans

Lüfterdaten werden von den Lüftersensoren abgerufen/generiert und sind mit der *CDiagReport.h*-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<Fans Schema="1" Count="2">
   <Fan Name="FAN1 SYS" CSS="true">
      <Status Description="not manageable">5</Status>
   </Fan>
   <Fan Name="FAN PSU" CSS="false">
      <Status Description="not manageable">5</Status>
   </Fan>
</Fans>
```

#### 12.3.2.7 Temperature

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<Temperatures Schema="1" Count="7">
   <Temperature Name="Ambient" CSS="false">
      <Status Description="ok">6</Status>
      <CurrValue>27</CurrValue>
      <WarningThreshold>37</WarningThreshold>
      <CriticalThreshold>42</CriticalThreshold>
   </Temperature>
   <Temperature Name="Systemboard" CSS="false">
      <Status Description="ok">6</Status>
      <CurrValue>37</CurrValue>
      <WarningThreshold>60</WarningThreshold>
      <CriticalThreshold>65</CriticalThreshold>
   </Temperature>
…
```

#### 12.3.2.8 Power Supplies

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<PowerSupplies Schema="1" Count="1">
   <PowerSupply Name="PSU" CSS="false">
      <Status Description="ok">1</Status>
   </PowerSupply>
</PowerSupplies>
```

#### 12.3.2.9 Voltages

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<Voltages Schema="1" Count="11">
   <Voltage Name="BATT 3.0V" CSS="false">
      <Status Description="ok">1</Status>
      <CurrValue>3.24</CurrValue>
      <NomValue>3.00</NomValue>
      <Thresholds>
         <MinValue>2.02</MinValue>
         <MaxValue>3.50</MaxValue>
      </Thresholds>
   </Voltage>
```

#### 12.3.2.10 IDPROMS

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Darüber hinaus wird der aus dem FRU SDR-Datensatz abgerufene tatsächliche Name als Attribut "Name" im Instanz-Tag angegeben. Da ein Eintrag relativ lang ist, überprüfen Sie eine generierte Datei, um ein Beispiel zu erhalten.

#### 12.3.2.11 SensorDataRecords

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Da ein Eintrag relativ lang ist, überprüfen Sie eine generierte Datei, um ein Beispiel zu erhalten.

#### 12.3.2.12 PCIDevices

Der iRMC hat keinen direkten Zugriff auf die PCI-Daten und kann daher nur eine begrenzte Teilmenge an Informationen angeben. Diese Informationen basieren darauf, was das Server-BIOS mit dem OEM IPMI-Befehl F119 gesendet hat und was mit dem OEM IPMI-Befehl F11A abgerufen werden kann. Beispielausgabe siehe unten.

```
<PCIDevices Schema="1">
   <Device>
      <ConfigSpace>
         <VendorId>1000</VendorId>
         <DeviceId>005B</DeviceId>
         <SubVendorId>11D3</SubVendorId>
         <SubDeviceId>1734</SubDeviceId>
```

```
         <BaseClass>Mass storage controller</BaseClass>
         <SubClass>RAID controller</SubClass>
      </ConfigSpace>
      <Slot>4</Slot>
   </Device>
</PCIDevices>
```

#### 12.3.2.13 SystemEventLog

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<SystemEventlog Schema="1">
   <Entry>
      <Date>2014/02/05 16:48:13</Date>
      <Severity>MINOR</Severity>
      <ErrorCode>19000B</ErrorCode>
      <Message>'DIMM-1B': Non Fujitsu Memory Module detected -
Warranty restricted!</Message>
      <Data Size="14">
         <HexDump Lines="1" BytesPerLine="14">
            <Line Offset="0">
               <Hex>02 4D 6B F2 52 20 00 04 E1 FE 6F A0 00
03</Hex>
            </Line>
         </HexDump>
      </Data>
   </Entry>
…
```

#### 12.3.2.14 InternalEventLog

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<InternalEventlog Schema="1">
   <Entry>
      <Date>2014/02/05 15:53:00</Date>
      <Severity>INFO</Severity>
      <ErrorCode>23000B1</ErrorCode>
      <Message>iRMC S4 Browser http connection user 'admin'
login from 10.172.103.28</Message>
   </Entry>
…
```

#### 12.3.2.15 BootStatus

Die generierten Informationen sind mit der *CDiagReport.h*-Implementierung kompatibel. Beispielausgabe siehe unten.

```
<BootStatus Schema="1">
   <PowerOnReason AsString="Power Switch">1</PowerOnReason>
   <PowerOffReason AsString="Software">0</PowerOffReason>
   <PowerFailBehavior AsString="remain
off">1</PowerFailBehavior>
</BootStatus>
```

#### 12.3.2.16 ManagementControllers

Es werden nur Informationen über den iRMC S4-Host angegeben.
Beispielausgabe siehe unten.

```
<ManagementControllers Schema="1">
   <iRMC Name="iRMC S4">
      <Firmware>97.30F</Firmware>
      <IPAddress>10.172.103.13</IPAddress>
      <IPSubnetMask>255.255.255.0</IPSubnetMask>
      <IPGateway>10.172.103.1</IPGateway>
      <MACAddress>00-19-99-FD-AF-9F</MACAddress>
      <ManagementLANPort>0</ManagementLANPort>
      <IPNominalSpeed>0</IPNominalSpeed>
   < iRMC>
<ManagementControllers>
```